# Crisis Management and Recovery for Events: Impacts and Strategies (2021)

Ziakas,V. Anchak, V. and Getz, D. (editors)

## Chapter 3

## From Risk to Resilience: Contemporary Issues in Event Risk Management

Peter Ashwin

## Abstract

In today's volatile, uncertain, complex and ambiguous global risk society, event organizers and event professionals find themselves planning and delivering festivals and events in a dynamic environment characterized by the disruptive effects of the covid-19 pandemic and extant risks from homegrown violent extremism, cyber-criminal threats, supply chain disruptions and event cancellations (Hall, 2018; Piekarz et al, 2015; Reid and Ritchie,2011; Rutherford Silvers, 2008; Tarlow, 2002, Beck, 1999).  Drawing upon the existing body of literature for event risk management, from Berlonghi (1990) to a recent 2019 industry survey on event risk management practices (Ashwin and Wilson, 2020), this chapter explores contemporary risk issues in today's volatile, uncertain, complex and ambiguous world. The first section of the chapter delves into the inter-related risk constructs for the socio-cultural theoretical perspectives of risk, focusing on how an event organizers perception of risk influence their approach to risk management and decision-making? The second section of the chapter then goes on to explore in depth, two contemporary, high impact organizational and security risks: first, the cyber-criminal threat to event digital eco-systems; and second, domestic terrorism, the evolving threat from homegrown violent extremists, domestic violent extremists and 'lone wolves.  Following on, new perspectives and insights into risk mitigation and event resilience are outlined; the utilization of situational crime prevention, an evidence-based criminology perspective and other 'real world' opportunities for event organizers to enhance event team preparedness and resilience to adversity and uncertainty.

How to Cite: Ashwin, P. (2021) 'From Risk to Resilience: Contemporary Issues in Event Risk Management' in Ziakas,V. Anchak, V. and Getz, D. (Eds) *Crisis Management and Recovery for Events.* Oxford: Goodfellow Publishers Limited.

# 3 From Risk to Resilience: Contemporary Issues in Event Risk Management

***Peter Ashwin***

> *Our brains tend to go for superficial clues when it comes to risk and probability, these clues being largely determined by what emotions they elicit or the ease with which they come to mind*
>
> Nassim Nicholas Taleb

## Introduction

In today's volatile, uncertain, complex and ambiguous global risk society, national boundaries are blurred, inter-connected markets are exposed to delocalized risks with consequences that may stretch over extended or indefinite periods of time. Under these uncertain conditions, event organizers find themselves planning and delivering events in an environment characterized by disruptive effects of the Covid-19 pandemic and extant risks from home-grown violent extremism, cyber-criminal threats, supply chain disruptions and event cancellations (Beck, 2006; Hall, et al., 2019; Piekarz et al., 2015; Reid & Ritchie,2011; Rutherford Silvers, 2008; Tarlow, 2002).

It is widely acknowledged that risk management should be viewed by event organizers and event professionals as a fundamental responsibility for planning and delivering a world class guest experience in a safe and secure environment (Berlonghi, 1990; Piekarz et al., 2015; Rutherford Silvers, 2008; Tarlow 2002;). However, in stark contrast, many event organizers concede that they do not have an event risk management plan (Ashwin & Wilson, 2020; Sturken, 2005 cited in Robson, 2009; Robson, 2009). In light of the recent proliferation of violent attacks on festivals and events, from the 2013 Boston Marathon bombing to the recent 2019 Gilroy Garlic Festival (California) shooting, there has been an increasing public discourse and emerging legislative requirements for event organizers to demonstrate an evidence-based approach to risk management decisions with the ability to explain the rationale behind those decisions in clear, objective and transparent terms (US Department of Homeland

Security, 2020; UK Center for the Protection of National Infrastructure, 2020).

Drawing upon the existing body of literature for event risk management, from Berlonghi (1990) to the recent 2019 event industry survey investigating event organizers approaches to risk management and resilience (Ashwin & Wilson, 2020), this chapter will explore contemporary risk issues in today's volatile, ambiguous, complex and uncertain world. First, it will discuss the inter-related risk constructs pertaining to socio-cultural theoretical perspectives of risk and how an event organizer's perception of risk influences their approach to risk management and decision-making. Then the chapter will address two contemporary risks, both of which present the potential for catastrophic consequences: cyber-criminals who are increasingly focusing their cyber-attacks on vulnerable, event digital eco-systems; and domestic terrorism and the threat from homegrown violent extremists, domestic violent extremists and unaffiliated lone offenders ('lone wolves'). Finally, pragmatic, risk-based approaches to mitigating these risks will be discussed, specifically, preventative risk control measures and opportunities for enhancing organizational resilience to cyber-crime and terrorism.

## The perception of risk: Making sense of the risk management construct

> *…risk cannot be eliminated: there will be incidents, so we must focus on resiliency under all conditions…*
> Caitlin Durkovic[1]

In order to understand the approach an organizer adopts for managing risks to their event or organization, one must first explore the phenomenon of the perception of risk. This has been theorized in social scientific literature through three major theoretical perspectives: (1) the naïve realist or techno-scientific, (2) cognitive psychology and (3) sociocultural (Lupton, 2013). The techno-scientific perspective contends that risk is a product of a hazard or threat (risk source or trigger), measured through the calculations of likelihood and the consequences, an underlying premise, which is consistent with the International Standards Organization *ISO 31000 (20018) Risk Management – Guidelines*. Techno-scientific theorists also argue that the layperson's, reliance on intuition and their perceived lack of risk knowledge and subjective approach, results in inferior decisions and responses as compared to a techno-scientific perspective (Lupton, 2013). Beck (1999), however, contends that one should not have to choose between a natural-scientific objectivism (naïve realist) or a cultural relativism (subjective) approach for risk management, but rather use each when it is appropriate to understand the complex

[1] Assistant Secretary, Infrastructure Protection, US Department of Homeland Security, 2016

and ambivalent nature of the risk environment. This position is supported by the social-constructionist argument that risk judgements are in part based on prior knowledge, personal embodied experiences, discussions with others and access to expert knowledge about how relevant industries and regulatory bodies have tended to deal with risk in the past (Lupton, 2013; Slovic, 2000).

Within the events context, risk perception has been described "*the concerns of the various entities involved in the event*" (Berlonghi, 1990, p. 19) and that the risks identified by the event organizers may not be accurate nor verifiable, particularly in the absence of an event risk assessment. An event organizer's perception of risk is not only based on perceptive or objective fact, but also by their background, experience, the organizational culture and the influence of the senior management team attitude to risk (Robson, 2009). Event organizers often rely on intuitive risk judgments based on a foundation of experience, which seldom incudes direct experience with the risk event but this in itself should not be considered erroneous or biased, if event organizers' opinions differ from that of expert risk assessments (Lupton, 2013; Rogers, 1997).

In summary, given the inherent limitations of risk-based decision-making within uncertain environments and the fundamental processes of human risk perception, it is clear that the subjective decision-making will always be part of the event risk assessment process (Talbot, 2011).

## Risk management: Current approaches and practices

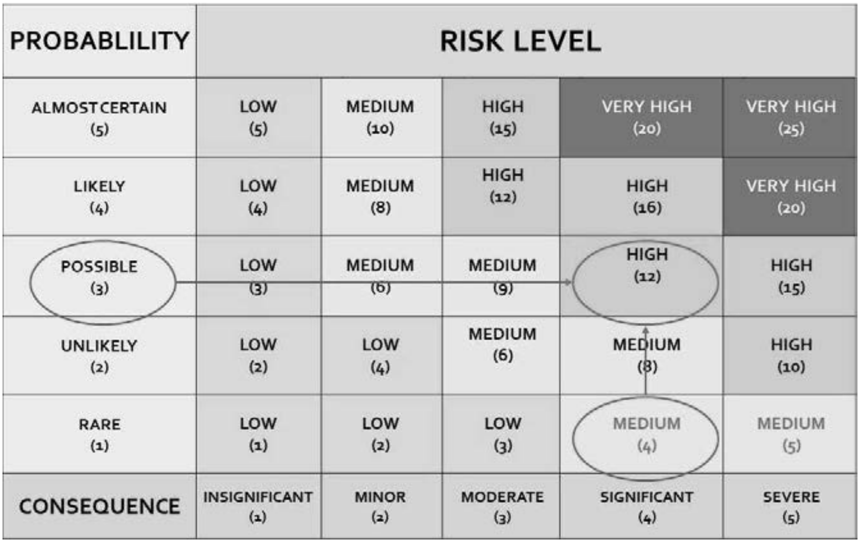
While there is a relatively large body of literature asserting that risk management is fundamental to planning and delivery of safe and secure events, there still remain gaps in research and literature specific to event organizers' approaches to risk management (Khir, 2014; Robson, 2009). Furthermore, the existing body of literature on risk management within the events industry focuses, in the most part, on insurance and legal obligations, vendor agreements, indemnifications, waivers and insurance policies, but not on the role of event managers and their responsibilities as operational risk 'owners' (Rutherford Silvers, 2008).

Berlonghi (1990) was amongst the first academic practitioners to highlight risk management as an integral part of the event management process: the process by which an event is planned, prepared and produced (Goldblatt, 2011; Rutherford Silvers, 2008). Within the events context, risk management can be described as the process of making and carrying out decisions that minimize the adverse effects of the potential losses of an event or simply stated as "*making events as safe and secure as possible*" (Berlonghi, 1990, p.3), or alternatively:

> "*a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for*

*managing risks that may hinder an organization from achieving its objectives"* (US Department of Homeland Security, 2011, p. 13)

Effective risk management requires the assessment of inherently uncertain events through two dimensions: (1) how likely is the risk event, and (2) what are the potential consequences (impacts) to the successful achievement of the organization's mission and objectives? The probabilistic risk assessment (PRA) is one of the most commonly used tools to quantify risk through an assessment of the aforementioned factors of likelihood (probability) and consequence to provide a risk estimate or rating, commonly referred to as the level of risk (Ostrom & Wilhelmsen, 2012). If sufficient rigor has been put into defining the context of the risk statement, the likelihood and the consequence metrics, then a meaningful risk estimate (risk rating) can be quickly and consistently obtained from a risk matrix (Talbot, 2011).



| PROBABLILITY | RISK LEVEL | | | | |
|---|---|---|---|---|---|
| ALMOST CERTAIN (5) | LOW (5) | MEDIUM (10) | HIGH (15) | VERY HIGH (20) | VERY HIGH (25) |
| LIKELY (4) | LOW (4) | MEDIUM (8) | HIGH (12) | HIGH (16) | VERY HIGH (20) |
| POSSIBLE (3) | LOW (3) | MEDIUM (6) | MEDIUM (9) | HIGH (12) | HIGH (15) |
| UNLIKELY (2) | LOW (2) | LOW (4) | MEDIUM (6) | MEDIUM (8) | HIGH (10) |
| RARE (1) | LOW (1) | LOW (2) | LOW (3) | MEDIUM (4) | MEDIUM (5) |
| CONSEQUENCE | INSIGNIFICANT (1) | MINOR (2) | MODERATE (3) | SIGNIFICANT (4) | SEVERE (5) |

**Figure 3.1:** Probabilistic risk assessment matrix (heat map)

Figure 3.1 provides an example of a risk matrix (heat map), typically referred to as a '5 x 5' risk matrix, where both probability (likelihood) and consequence are qualitatively described and quantitatively scored, for example the probability of occurrence 'almost certain' is rated as five, as opposed to 'rare' which is rated as one. The risk score or estimate is calculated by multiplying the assessed probability rating by the consequence rating.

Although semi-quantitative in nature, risk matrices provide a visual presentation of ranked risks which then allows event decision-makers to make value judgements to prioritize resource allocation to mitigate the risks to a level as low as reasonably possible (ALARP principle) or to fall within the designated risk appetite of the event senior management team (International Standards Organization, 2018; Hopkin, 2010).

Probability risk assessments are often viewed by event organizers as being an overly complex and challenging endeavor, given the requirement to construct likelihood and consequence metrics and risk level statements, and compounded by the fact that event organizers typically have limited risk management knowledge or experience. An alternative approach to event risk assessments, is ‘risk ranking’, a comparative, subjective risk assessment exercise to rank and prioritize management of risks within an organization (Hancock, 2019; Florig et al., 2001). Another advantage of the risk ranking exercise is that it provides team-based opportunities for all levels of event management to engage in risk discourse, fostering a heightened level of risk awareness and the opportunity for horizontal integration across typically, siloed event functional areas.

A risk ranking exercise for event organizing committee involves the following steps, the indicative outcome of which is summarized in Table 3.1.

1. Event senior management and the operational management team come together for a risk ranking workshop;
2. As a group, identify and collectively agree on a list of risks (risk register) which collectively ‘keep them up at night’; for the purpose of this example, the risk register is assumed to contain five risks;
3. Then each individual is asked to assign a numerical ranking value, one being for the lowest risk and five for the highest risk;
4. The scores per risk are added to provide an aggregated risk score;
5. Finally, the risk register is resorted/prioritized based on the final risk scores.

**Table 3.1:** Risk ranking exercise

| Risk Statement | #1 | #2 | #3 | #4 | #5 | Total Score | Risk Ranking |
|---|---|---|---|---|---|---|---|
| (1) Inability to attract, recruit and retain high caliber staff due to the disruption of Covid-19 pandemic | 5 | 4 | 3 | 4 | 3 | 19 | **1** |
| (2) Severe weather event triggers evacuation of event site and event cancellation | 2 | 2 | 1 | 3 | 2 | 10 | **5** |
| (3) Active assailant firearms attack inside the event site | 3 | 4 | 2 | 3 | 4 | 16 | **3** |
| (4) Disruption to IT network and data access due to cyber-criminal ransomware attack | 2 | 1 | 3 | 3 | 2 | 11 | **4** |
| (5) Ticket sales do not meet forecasted targets resulting in significant budget shortfalls | 3 | 5 | 4 | 2 | 3 | 17 | **2** |

One key point to note, is that agreement among participants is not, in itself, an objective of the risk ranking exercise because individual participants should be encouraged to disagree about the relative levels of risk based on their perception of risk.

Risk ranking offers event organizers an opportunity to add process to their subjective risk assessments to better inform future decision-making and communication of risk information within the organization. However, event organizers should remain cognizant of the fact that subjective risk assessments are prone to bias, error, the potential for over-estimation or under-estimation of risk, which may result in ill-informed decisions (Hillson, 2016; Lupton, 2013; Piekarz et al., 2015; Slovic & Peters, 2006).

If event organizers collected and analyzed statistical data from after-action reports, near misses and incident reports, this dataset provides opportunities to gain valuable risk insights to support objective and informed judgments for risk mitigation (Reason, 1990, 1997; Robson, 2009). This argument is supported by the findings from Ashwin and Wilson's (2020) survey into the event industry's risk management practices, eliciting 160 responses from festival and event leaders across 11 countries. Only 18% of the respondents indicated that they had a current risk management plan and 35% indicated they did not have a risk management plan and or, did not know if they had a plan. In the absence of personal or organizational experience with risk events, organizers and event professionals will look externally for opportunities to leverage accumulated risk management experience and knowledge from other event organizers and industry trade associations like the International Festival and Events Association (IFEA) to assess risk trends and frequency within the industry, gain insights into the severity of past risk events and to identify industry best practices for risk mitigation. Industry research also provides opportunities for event organizers to leverage information across the industry, for example, Figure 3.2 provides a summary of perceived risks versus actual risk events from Ashwin and Wilson's (2020) industry survey.

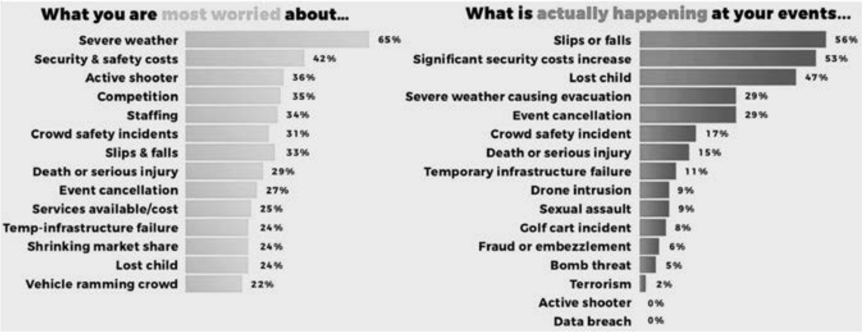


**Figure 3.2:** 2019 Event industry survey results: Perceived risk ranking versus actual risk events

The awareness and maturity of risk management within the events industry is undeniably growing as event managers migrate from an insurance-led approach to an event management led approach. However, it remains evident that the events industry faces ongoing challenges developing a mature level of capability to proactively manage event risks; be it subjective, value-based judgments through risk ranking or quantitatively through probability risk assessments. As an industry, we must continue to pursue further academic research into event risk management and to provide opportunities for professional development of our next generation of events leaders in risk management.

## Decision-making under uncertainty

Are event management decisions primarily driven by a deliberate and rational analysis or a more intuitive, heuristic-based approach? This section of the chapter will review theoretical approaches to decision-making under uncertainty and how the perception of risk may also influence event organizers' decision-making.

Klein's (1993, 1998) research on recognition prime decision (RPD) model concludes that decision-making is a perpetual process, situationally based to facilitate fast effective decision-making, based on previous experience and intuitive knowledge that enables the decision-maker to generate fast and effective courses of action. The recognition primed decision model reasons that fast, effective decision-making is possible within time critical situations when the decision-maker has the expertise and situational awareness, combined with a battery of experience-based, intuitive knowledge (Klein, 1993, 2008).

Event organizers often rely on intuitive risk judgments, known as heuristics (mental shortcuts) to make inferences and decisions based on what they individually and collectively remember observing or experiencing during previous risk events (Laybourn, 2003; Slovic, 2000). In contrast, rational theories of decision-making assume that decision-makers follow a rational procedure for making decisions, selecting the option that will produce the best outcome (Laybourne, 2003). Research into naturalistic decision-making (NDM) focused on how first responders utilized their expertise and experience to make effective decisions through utilizing systems of work known to have been successful in previous uncertain and high stress situations (Ash & Smallman, 2010). Slovic (2000) argues that people like event organizers may judge risks and hazards more efficiently, and make better decisions under pressure using heuristics rather than an analytical or systematic approach.

Event organizers will rarely have the necessary information and time for an analytical based decision-making process but under these conditions, naturalistic decision-making allows event organizers to leverage their expertise, experience and intuition to reach timely 'satisficing' decisions within dynamic and complex multi-agency environments (Klein, 1993, 2008; Tarlow, 2002). Yet conversely, 83 per cent of the 160 respondents from Ashwin's and Wilson's (2020) industry survey indicated that they had limited confidence in their event team 'mission readiness' and capability to respond and manage adverse events within volatile, ambiguous, complex and uncertain event environments.

## Decision support models: The OODA loop

Event organizers, like other professionals, have great difficulty making decisions and judgements under uncertainty and operating environments characterized by multiple situational inputs (Plous, 1993). An event organizer's decision-making can be improved through adopting a repeatable and systematic decision-making model; one such model which is applicable to the events environment, is the 'observe, orient, decide and act' decision-making model, otherwise known as the OODA loop (Boyd, 1979). Developed in 1979 by United States Air Force Colonel John Boyd, the OODA Loop comprises four interrelated, multi-dimensional elements: observation, orientation, decision and action, which encompass both time and space (Rule, 2013).

Adopted from Boyd's OODA loop, Figure 3.3 provides a simplified but structured checklist approach to support decision-making under uncertainty by event organizers and their operational management team. This model has improved effective decision-making by event professionals from team supervisors to senior management.

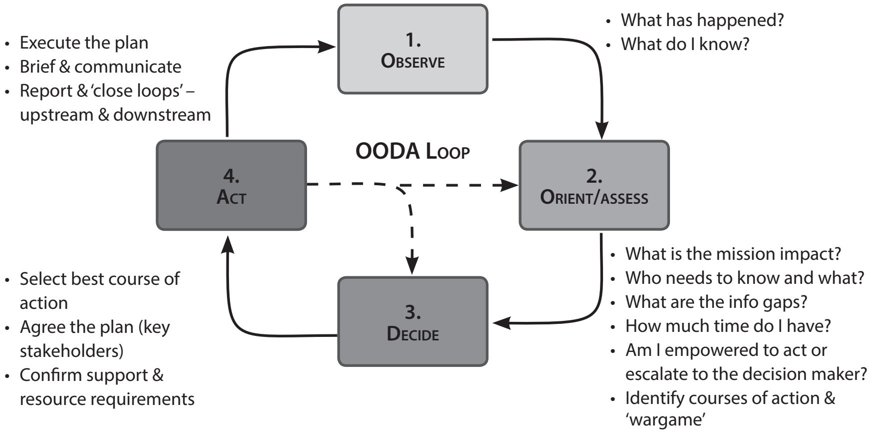

1. Observe
2. Orient/assess
3. Decide
4. Act
OODA Loop
• What has happened?
• What do I know?
• What is the mission impact?
• Who needs to know and what?
• What are the info gaps?
• How much time do I have?
• Am I empowered to act or escalate to the decision maker?
• Identify courses of action & 'wargame'
• Select best course of action
• Agree the plan (key stakeholders)
• Confirm support & resource requirements
• Execute the plan
• Brief & communicate
• Report & 'close loops' – upstream & downstream

**Figure 3.3:** Decision support methodology for event organizers – the OODA Loop

# The emergence of domestic terrorism threats

## An evolving threat landscape

Since 9/11, the threat of terrorism and targeted violence against vulnerable soft targets and mass gatherings (festivals and events) remains one of the most serious risks to the United States homeland security (Department of Homeland Security [DHS], 2020). The current threat landscape highlights the proliferation of home-grown violent extremism and domestic violent extremism, giving rise to new configurations of low capability, high impact, asymmetric attacks utilizing firearms, edged weapons, vehicles as weapons, and improvised explosive devices to violently attack soft targets as evidenced by the attacks on the Boston Marathon, 2013; the Pulse nightclub, 2016 (Orlando); Route 91 Harvest Country Music Festival, 2017 (Las Vegas), Ariana Grande Concert, 2017 (Manchester, UK) and the Gilroy Garlic Festival, 2019 (California). Accessible, crowded, mass gatherings like festivals and events will continue to remain attractive targets for various threat actors into the foreseeable future (DHS, 2020; Hesterman, 2015).

Terrorism in today's global risk society is a complex problem. It is widely recognized that the underlying causes of terrorism and other forms of violent extremism are manifested through many sources of conflict, including ethnic, religious, political, economic and ideological influences which may accelerate an individual's pathway to radicalization or extremism (Clarke & Newman, 2006). Post-modern domestic terrorism is often characterized as a leaderless resistance, where individuals and groups connect through a shared ideology enabled through the internet without any defined leadership (Hesterman, 2015). Understanding the pre-conditions and precipitants that trigger a terrorist or violent lone offender to embark on a pathway to violence, provides an opportunity for event organizers, the private security sector and law enforcement to apply a targeted, risk-based security counter measures (risk controls) to reduce terrorism related risks. A risk-based approach identifies security countermeasures to reduce the likelihood of a terrorist attack occurring (deter and detect) and in the event of a terrorist attack, identifying response and recovery measures to reduce the severity of the consequences to people, property and reputation (Bjorso & Silke, 2019).

The 2020 US Department of Homeland Security threat assessment for mass gatherings assesses the three primary threats to events: (1) lone offenders who lack a clearly discernible political, ideological or religious motive; (2) small cells of individuals categorized as domestic violent extremists, motivated by racial or anti-authoritarian factors to commit unlawful acts of violence; and (3) homegrown violent extremists inspired by, or directed by foreign terrorist organizations to engage in ideologically motivated, terrorist activities (DHS, 2020).

The evolving sophistication and adaptive capability of terrorists, criminals and other malicious threat actors is routinely underestimated (Hesterman, 2015; Mcllhatton, et al., 2019). Threat actors adapt their tactics based on the lessons learnt from the successes and failures of other terrorist attacks, both domestically and internationally (Haberfeld & von Hassell, 2011). Furthermore, the internet enables exchange of secure web-based global conversations over the 'dark web' and social media channels between disconnected, like-minded individuals and other virtual communities, to share and acquire the know-how to execute highly lethal attacks on soft targets (Bouhana et al., 2018; Mcllhatton et al., 2019). Terrorist attacks are rarely sudden and impulsive; a terrorist's or other threat actor's ability to modify and adapt their tactics to the target environment should not be underestimated, nor should there be an over reliance on past events to predict the probability of future attacks (Clarke & Newman, 2006; Hesterman, 2015).

A successful terrorist attack is catastrophic – substantial loss of life, property damage, severe financial loss and irreparable reputational harm to the organization and its executive leadership (Mcllhatton et al., 2019). Recent low sophistication attacks in the US are frequently characterized by the use of firearms as opposed to other methods, where little or no training expertise (capability) is required and can be easily and inexpensively acquired (Bouhana et al., 2018). This is evidenced by two recent lethal attacks within the events industry: the 2016 Pulse nightclub terrorist attack in Orlando resulting in 49 fatalities and 53 wounded patrons (Ellis et al., 2016) and the 2017 Harvest 91 Country Music Festival resulting in 58 fatalities and a 2020 settlement of $800 million for the victims of the shooting by MGM Resorts (Ferrara, 2020). Event organizers have a legal responsibility and duty of care obligation to provide a safe environment and reduce the potential of harm from foreseeable risks for their guests, workforce and other client groups/stakeholders who attend their events (Clark & Saviour, 2018).

## Reducing terrorism risks through situational crime prevention

Terrorism risks to events and mass gatherings cannot be eliminated, however, a risk-based approach provides opportunities to enhance an event's security posture, preparedness and resilience to known terrorist threats. Terrorism risk can be defined as a function of threat, vulnerability, and consequence; where the existent threat and the inherent vulnerabilities of the organization represent the 'likelihood' that an attack will be successful (Willis, 2007). By identifying potential threats and assessing potential vulnerabilities when exposed to known threats, appropriate risk controls (security counter measures) can be identified and aligned to available resources within predetermined budgets (Ezell et al., 2010).

Given the inherent uncertainty of terrorism risks and the difficulty to assess the level of terrorism risk with a high level of confidence (Aven & Renn, 2009), an alternate approach to mitigating terrorism risk was postulated by Clarke and Newman (2006) to utilize situational crime prevention (SCP) principles to reduce the risk of a terrorist attack. Underpinned by two criminological theoretical perspectives, rational activity theory and rational choice theory, Clarke and Newman's (2006) seminal SCP publication, *Outsmarting the Terrorists*, provides a pragmatic and effective approach for counterterrorism through five SCP strategies: (1) increasing the effort, (2) increasing the risks, (3) reducing the reward, (4) reducing provocation and (5) removing excuses. Table 3.2 provides examples for SCP that can be applied by event organizers and their security partners to enhance the event security and resilience.

**Table 3.2:** The counter terrorism application of SCP for events

| SCP Principle | Event based examples |
|---|---|
| (1) Increase the effort | Increasing the difficulty for a threat actor during pre-attack surveillance or final dry rehearsals, provides opportunity to disrupts their attack vector pathway. |
| (2) Increase the risk | Increase the risk of detection and detainment through highly visible police presence, security patrols and an event workforce who have enhanced security and situational awareness for reporting suspicious activity (training). |
| (3) Reduce the reward | Reducing the reward involves implementing strategies that make the target less attractive or reducing the gain or pleasure from executing the attack. For events, this attribute is closely aligned to increasing the risks and increasing the effort. |
| (4) Reduce provocation | While not directly applicable to counter terrorism for event per se, reduced provocation strategies provide opportunities to de-escalate situations before they trigger public safety or criminal situations, for example, 'verbal judo' techniques to de-escalate situations with non-compliant guests. |
| (5) Remove excuses | Removal of excuses through the use of signage, terms and conditions of entry, prohibited and restricted items policies, makes it difficult for offenders or threat actors to use excuses for their behavior, for example unauthorized access into controlled or restricted areas. |

In summary, SCP attempts to shape, influence, or intervene in the terrorists or criminal offenders decision-making process by influencing environmental opportunities that reduce the attractiveness of the target and increase the perceived risk of being caught.

## EVIL DONE: Reducing terrorism risk through 'thinking like a terrorist'

Terrorist decision-making and target selection is largely governed by environmental opportunities and constraints in relation to planning, capabilities and resources (Freilich et al., 2019). Through understanding a terrorist's decision-making criteria for target selection, the attractiveness of an event as a potential terrorist target can be evaluated, inherent vulnerabilities identified and reduced, and opportunities identified to enhance the resilience and preparedness of the event team's capability to respond and recover from a terrorist incident.

To identify effective counter terrorism measures, event organizers must think like a terrorist. Adopting a threat actor's targeting mindset, allows event organizers to subjectively assess their event's attractiveness and vulnerability to a terrorist attack, where vulnerability refers to the "*inherent features of the target that are more susceptible or attractive to attack by terrorists*" (Clarke & Newman, 2006, p. 90). Clarke and Newman (2006) theorized that the terrorist target selection was based on a combination of eight attractiveness criteria, according to whether the potential target was: exposed, vital, iconic, legitimate, destructible, occupied, near, and easy; summarized by the acronym 'EVIL DONE'. Terrorist target pre-selection is conditioned by a combination of these factors; more vulnerable targets possess a greater number of these attributes (Boba, 2009). Table 3.3 provides a practical approach for event organizers to subjectively assess the attractiveness and vulnerability of their event to a terrorist threat through EVIL DONE.

## Risk-based counter terrorism strategies for events

Terrorists and other threat actors plan attacks in observable stages which include the conduct of initial target surveillance, pre-attack surveillance (hostile reconnaissance) and final dry rehearsal before initiation of the attack. Through understanding the planning stages of a hostile event or terrorist attack, event organizers have the opportunities to deter and detect potential terrorist attacks and other criminal activities through risk-based counter measures to increase the threat actors' efforts required and their likelihood of detection or discovery during the attack planning cycle (Anarumo, 2011; Clarke & Newman, 2006; DHS, 2019; US National Counterterrorism Center, 2020).

Table 3.4 provides examples of applied counter terrorism, event security measures based on risk-based principles: (1) preventative risk control measures (deter, detect and delay) which reduce the likelihood of a terrorist attack through increasing the effort and risk; and (2) responsive risk control measures (respond and recover) designed to enhance the preparedness and resilience of event workforce to respond confidently and effectively in a post terrorist incident environment.

**Table 3.3:** EVIL DONE: Event attractiveness and vulnerability target attributes

| EVIL DONE | Event attractiveness and vulnerability target attributes |
|---|---|
| **E**xposed | Visible, exposed target (event site or venue), easily accessible for pre-attack surveillance and dry rehearsals by the threat actor. |
| **V**ital | Police and security patrols, enhance workforce security awareness and suspicious activity reporting (training). |
| **I**conic | The iconic attribute considers the target's symbolic value to the terrorist or threat actor. Other iconic characteristics include whether the event highly recognizable – locally, regionally, or nationally through mainstream media and social media platforms. |
| **L**egitimate | Target is perceived as appropriate to attack, demographics and attendance by a specific individual /s may influence the selection of the target by the threat actor. |
| **D**estructible | Requires the least amount of effort, security is perceived to be ineffective, weapon choice and tactics offer opportunities for mission 'success'. |
| **O**ccupied | Terrorists are attracted to events with large, high density crowds within confined spaces to provide opportunities for enhanced lethality. |
| **N**ear | Terrorism is a local event; proximity and familiarity with the intended target and terrain requires less pre-attack preparatory efforts by the threat actor. Criminological research demonstrates that most terrorists and criminal offenders select targets close to home (within 50 miles) or where their routine activities take them (Freilich et al., 2019). |
| **E**asy | An event site or venue location characterized by requiring minimum effort and logistical support, easy accessible approaches to the target and a range of options for escape and evasion. |

While events and other gatherings will continue to remain attractive targets for various threat actors into the foreseeable future, it is possible for event organizers to reduce the risk of a terrorist attacks through counter terrorism solutions that are cost-effective, feasible and offer opportunities for enhancing an event team's resilience and capability to respond and recover from a critical incident through training and pre-event operational readiness and preparedness exercises.

**Table 3.4:** Counter terrorism risk reduction strategies for events

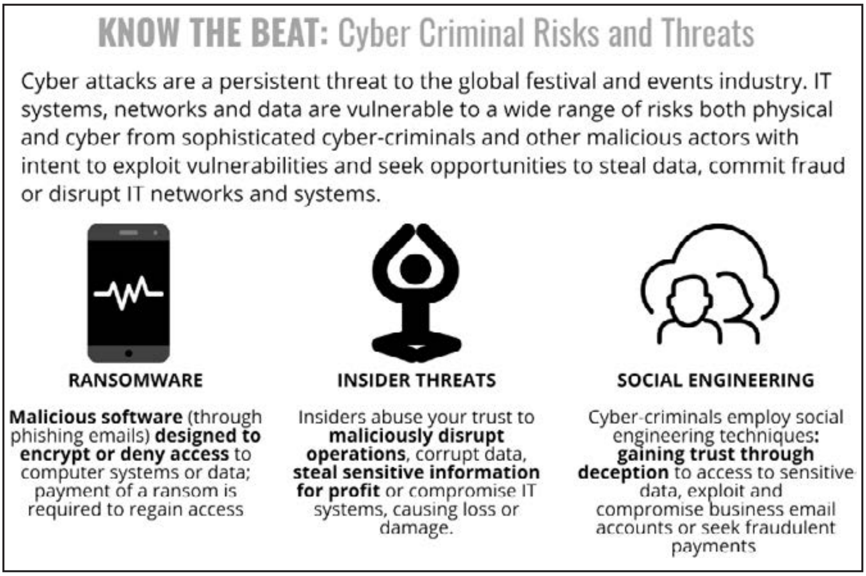
| Preventative Risk Control Measures |
|---|
| Event Security and Safety management Plan (ES2MP) – a comprehensive and tested, security and safety management plan is a matter of good business and corporate responsibility (DHS, 2019). |
| Electronic surveillance systems e.g., CCTV cameras, where budget allows - technology should complement other human-based security measures as opposed to be the focus of the counterterrorism effort (Hesterman, 2015). |
| Deployment of highly visible police and private security patrols, pre-event and during the event. |
| Implement a security awareness training plan to enhance individual and collective capabilities to identify pre-attack surveillance indicators and reporting suspicious behaviors and activities. |
| Background checks as an employment / volunteer pre-condition to reduce the risk of insider threats. |
| Responsive Risk Control Measures |
| Conduct pre-event tabletop exercises to exercise and validate emergency response plans with security and safety stakeholders and active shooter training drills with local law enforcement. |
| Provide traumatic first aid training 'stop the bleed' for frontline staff and budget for, and purchase an appropriate number of 'bleed control kits' for the event staff as part of the medical plan. |
| Conduct pre-event emergency response drills with front line staff including risk-based scenarios for active assailant, multiple casualty incident and evacuation. |
| Pre-event testing of unified command, control and communications (C3) arrangements between the event operations team, law enforcement and event security. |
| Critical Incident Medical Plan. |

## Cyber-criminal risks and digital age of events

The transformative effect from the advent of computers in the 1980s and the subsequent launch of the world wide web in the 1990s, has led to the evolution of today's digital society and the unprecedented reach of digital technology and computer networks within the events industry (Stratton et al., 2016). Furthermore, the rapid onset of the digital age also created unprecedented opportunities for increasingly, sophisticated, and capable cyber-criminals and cyber-deviant entrepreneurs to engage in low risk, high return, cyber-crimes (Levi et al., 2017). The relative ungovernability of cyberspace and the revolutionary developments in technology, present a multi-dimensional challenge for information security professionals and law enforcement agencies pursuing the prosecution of cyber-criminals across a globally inter-connected network, where national borders and jurisdictions are no longer distinct or defined (Cavelty, 2018; Chang & Grabosky, 2014; Stratton et al., 2016).

CYBER SECURITY:
Stay lost in the music,
not in the cloud
Cyber resilience for festivals & events in today's uncertain world

Cybersecurity risks are a persistent and serious threat to the events industry digital ecosystems (Figure 3.4). Event organizers are highly dependent on secure and uninterrupted access to information and communication technology (ICT) networks to service their e-commerce operations, social media marketing, and data management tools from their 'business as usual' workplaces as well as temporary event sites, where thousands of attendees will expect uninterrupted, high quality access to event ICT networks for e-commerce, social media and other event related digital information (Hindduja & Kooi, 2013; Lakhani, 2017; Levi et al., 2017). Cybercriminals are agile, adapt and continuously evolve their tactics, techniques, and technologies to target and exploit the events industry ICT systems whose cyber-defenses are known to be far more vulnerable and less sophisticated than those of larger organizations.



KNOW THE BEAT: Cyber Criminal Risks and Threats

Cyber attacks are a persistent threat to the global festival and events industry. IT systems, networks and data are vulnerable to a wide range of risks both physical and cyber from sophisticated cyber-criminals and other malicious actors with intent to exploit vulnerabilities and seek opportunities to steal data, commit fraud or disrupt IT networks and systems.

RANSOMWARE

**Malicious software** (through phishing emails) **designed to encrypt or deny access** to computer systems or data; payment of a ransom is required to regain access

INSIDER THREATS

Insiders abuse your trust to **maliciously disrupt operations**, corrupt data, **steal sensitive information for profit** or compromise IT systems, causing loss or damage.

SOCIAL ENGINEERING

Cyber-criminals employ social engineering techniques: **gaining trust through deception** to access to sensitive data, exploit and compromise business email accounts or seek fraudulent payments

**Figure 3.4:** Cyber criminal threats to events

## Cybercrime and its impact on the events industry

The concepts of cybercrime and cybersecurity have been in common usage throughout the public and academic domains since the 1990s; however, there still remains a limited consensus among criminologists on how cybercrime should be defined and how it can classified and aligned to criminal behavior within cyberspace (Gordon & Ford, 2006; Levi et al., 2017; McGuire & Dowling, 2013; Wall, 2001). Despite this lack of consensus, cybercrime has been described as any criminal offence that is specifically facilitated or committed using a computer, network, or hardware device or which has occurred in cyberspace (Chang & Graborsky, 2014; Gordon & Ford 2006). The question of how cybercrime could be classified and aligned to criminal behaviors and offences was largely unanswered by criminologists until Wall's (2001) seminal research into cybercrime. Wall's (2001) cybercrime typology consists of four categories aligned to harmful behavior rather than specific offenses:

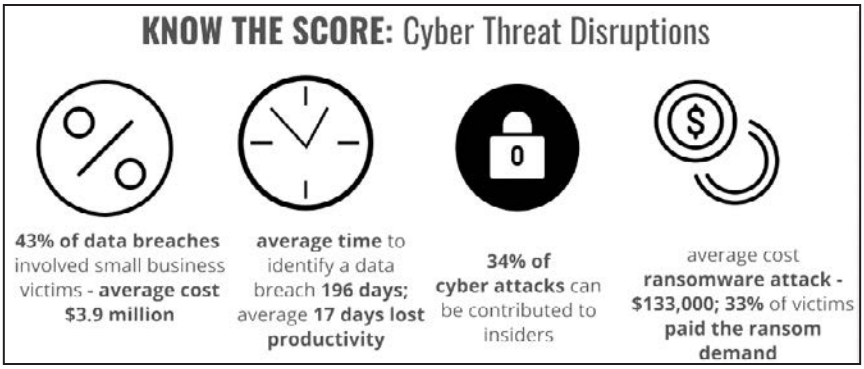
- cyber-trespass (unauthorized access to data through hacking and malware);
- cyber-deception (the use of social engineering, malware, identify fraud and fraudulent scams);
- cyber-porn and obscenity; and
- cyber-violence (the ways and means through which individuals can bring interpersonal harm to others through the web).

Measuring the impacts and cost of cybercrime within the events industry is problematic for the followings reasons: first, there is a limited body of evidence from official crime surveys and statistics; second, under-reporting of offenses by victims and an inherent lack of understanding that cybercrime is an offense; third, inconsistencies in terminology, reporting and victim survey methodologies; fourth, cybercrime has been commonly used to describe a general range of criminal offences; and fifth, the lack of harmonized statutes and legislation between national and international jurisdictions, particularly given the trans-jurisdictional nature of cybercrime, whereby the victim, the offender and the impact of the offense may reside in different jurisdictions (Chang & Grabosky, 2014; Furnell et al., 2015; Levi et al., 2017; McGuire & Dowling, 2013; Stratton et al., 2017; Wall, 2001).

The events industry sector encompasses a diverse range of activities that includes festivals, parades, meetings, conventions, expositions, sport and other special events, planned, coordinated and executed by the event organizing committee; typically categorized as a not-for-profit small business with fewer than twenty paid staff (Goldblatt, 2011; Getz, 1997). Cybersecurity risks are uniquely challenging for the event industry sector, for not only do event organizers have to protect their 'business as usual' workplaces from cybercrime threats, but they must also protect ICT systems at temporary event sites, where thousands of attendees will access event ICT networks for e-commerce, social media and to access other event related digital information (Lakhani, 2017).

While there is a limited body of literature pertaining to cybercrime and its impact on the events industry sector, complementary evidence can be derived from 'like industry' sector cybercrime surveys and reports, including the Verizon (2020) Data Breach Information Report; the UK Federation of Small Business report (2016) Cyber Resilience: How to Protect Small Firms in the Digital Economy; UK Government Department for Digital, Culture, Media and Sport (2019) Cyber Security Breaches Survey; and the Australian Cyber Security Center (2020) Cyber Security and Australian Small Business report. However, it should be noted that while surveys do not measure criminal activities or police reported crimes, they do provide indicators and insights into cyber-enabled and cyber-dependent crime datasets (McGuire & Dowling, 2013).

Recent research into the cybercrime impacts by Verizon (2020) and the UK Department for Digital, Culture, Media and Sport (2019) on small businesses (comparable to event organizing committees) indicates 32 per cent have experienced cyber security breaches or attacks. The research indicates that the most common types of attacks were phishing and others impersonating an organization in emails for fraudulent, financial gain and malware including ransomware. The infographic depicted in Figure 3.5, provides a summary of key facts and figures from the research.



**KNOW THE SCORE:** Cyber Threat Disruptions

**43% of data breaches** involved small business victims - **average cost $3.9 million**

**average time** to identify a data breach **196 days;** average **17 days lost productivity**

**34% of cyber attacks** can be contributed to insiders

average cost **ransomware attack - $133,000; 33%** of victims **paid the ransom demand**

**Figure 3.5:** A summary of cyber threat disruptions

## Data theft and malware – is your event at risk?

Data theft, a cyber-enabled crime, and malware, a cyber-dependent crime, are recognized as two of the most prevalent forms of cyber-attack vectors (Levi, et al., 2017; UK Dept. for Digital, Culture, Media and Sport, 2019). Data theft is an exploitation attempt by cybercriminals to obtain and exploit personal identifiable information (PII) for personal profit or financial gain through the use of technology, detailed online searches for personal information or social engineering techniques (Furnell et al., 2015; McGuire & Dowling, 2013). Within the UK arts, entertainment and recreation sector, 11 per cent of businesses reported being a victim of data theft. A recent high-profile event industry cyber-incident was the 2017 Coachella Valley Music and Arts Festival (Indio, California) reported a data breach involving 950,000 attendee PII records (Mercury News, 2017). It was subsequently reported that the Coachella attend PII accounts were being sold on the Dark Web for $300, presumably for targeted phishing campaigns (Hackread, 2017). While the financial and reputational cost from this data breach is unknown, it can be assumed to be significant; based on the average cost of USD $150 per record to compensate for consulting and legal services, restitution to victims, regulatory fines and recovery technologies (IBM Security 2020; Verizon, 2020).

The second prevalent cyber-dependent crime, malware, is software specifically designed to disrupt, damage or gain unauthorized access to computer systems. Its use by cybercriminals is primarily motivated by personal profit or financial gain (US Cybersecurity and Infrastructure Security Agency, 2020). Destructive malware attacks have become increasingly more common in the workplace, a recent 2020 survey indicated that more than 35 percent of small business respondents reported daily phishing, spoofing, malware, ransomware 'exploitation attacks' or other daily email threats (IMB Security, 2020). Malware as a cyberattack vector provides cybercriminals and other malicious actors with a low risk, high reward opportunity as evidenced through 21 per cent of UK small businesses reporting being a victim of malware (UK Federation of Small Business, 2016).

## Cybercrime risk mitigation: A pragmatic approach for event organizers

The viability and success of events is predicated on secure ICT systems and maintaining the confidentiality, integrity and availability of proprietary information and customer data records, accomplished through an overarching information security framework (Andress, 2011; Hinduja & Kooi, 2013; Whitman & Mattford, 2005). Despite this, event organizers do not perceive their events to be an 'attractive and lucrative target' for cyber-criminals. However, contrary to this perception, recent cybercrime research indicates an increasing threat to the events industry from cyber-criminals and other malicious actors (Millaire et al., 2017; UK Federation of Small Business, 2016).

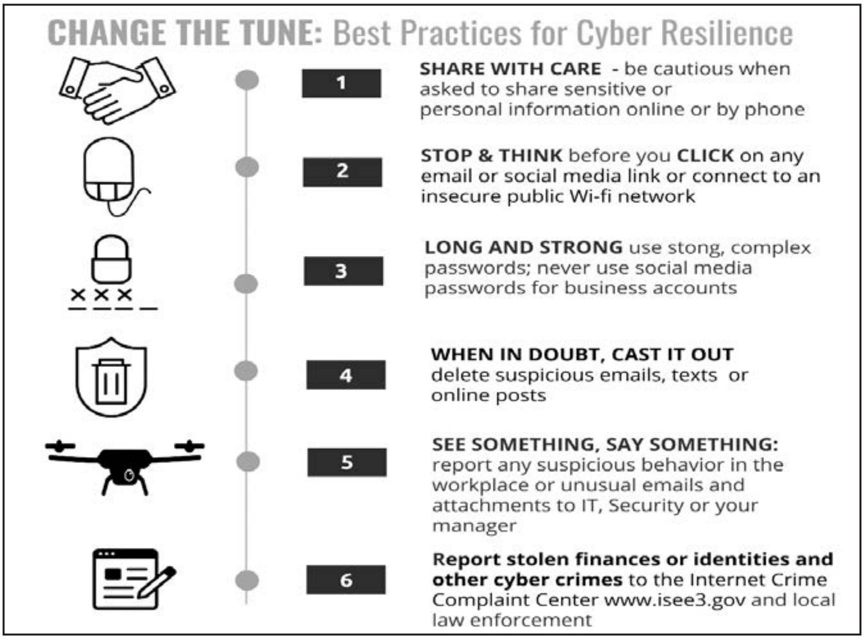
Recent arts and entertainment industry cybersecurity surveys indicated that 80 per cent of the sector (including event organizers) assessed their level of cybersecurity understanding as 'average' and their cybersecurity practices as 'below average' with an average cybersecurity investment of USD$2,600 per year (Australian Cyber Security Center, 2020; UK Department for Digital, Culture, Media and Sport, 2019). These findings provide valuable context, both financially and organizationally when considering the identification and selection of ‘fit for purpose’ cybercrime prevention and risk mitigation strategies for the events industry.

When considering the selection of cybercrime prevention strategies and other cybersecurity risk controls, foremost is the requirement to enhance the organizations IT security through a layered ‘defense-in-depth’ strategy and reduce technological organizational vulnerabilities, both internal and external (Cavelty, 2014; Whitman & Mattford, 2005). Furthermore, it should be recognized that event organizing committees like other small businesses, tend to be more vulnerable to technological and organizational weaknesses due to limited resources and capital, limited or no dedicated IT security staff, a lack of technical expertise and knowledge and conflicting business priorities (UK Federation of Small Businesses, 2016).

Considering the inherent cybersecurity vulnerabilities and the current levels of cyber-risk maturity of event organizers, the following cyber-security resilience measures provide a baseline for implementing a layered technical and organizational approach to information security, that is cost effective and sustainable. First, technological risk controls, including computer security software, data backed-up offsite or cloud based, regular updates of software and patches on all systems, secured wireless networks, encrypted data and communications capability, virtual private network. Second, organizational risk controls including strict password policy, security risk assessments at regular intervals, regular ICT system penetration tests, identify assurance/background checks on all employees, cyber insurance policy and cyber-incident business continuity plans.

Identifying cybersecurity best practices is only helpful if they are implemented by event organizers. So how do theoretical perspectives influence the likelihood of successful implementation of cybercrime prevention strategies? The application of criminological theories and other research perspectives provide an evidence-based methodology to inform the development of polices, practices, protocols and the overall approach to information security and crime prevention (Hinduja & Kooi, 2013). Insider threats account for 33 per cent of ‘cyberattacks’ and data breaches. Understanding this threat profile, the general deterrence theory (GDT) can be utilized to identify risk controls for the mitigating insider threats, for example, cybersecurity and password protection policies, access control and cybersecurity awareness training for staff (Lee et al., 2004). It has been contended that situational crime prevention (SCP) provides a better theoretical perspective than traditional theories for cybercrime prevention (Hinduja & Kooi, 2013). Applying SCP to the context of cybercrime prevention, seeks to reduce vulnerabilities through ICT system design, increase the risk/decrease the reward through criminal legislation and internal InfoSec policies, increase the effort by 'hardening' the digital ecosystem through ICT security protocols and encryption, and reduce the use of excuses (workforce and staff) through ICT cybersecurity policies and training.

The successful implementation of cybercrime prevention strategies within the events industry is likely, if cybersecurity measures are cost effective and can be easily implemented without unduly impacting on workplace productivity (Kirlappos et al., 2014). The Figure 3.6 infographic provides a visual example of best practices for cyber resilience of any event, regardless of size or whether, volunteer or staff led.



**CHANGE THE TUNE:** Best Practices for Cyber Resilience

1 **SHARE WITH CARE** - be cautious when asked to share sensitive or personal information online or by phone

2 **STOP & THINK** before you **CLICK** on any email or social media link or connect to an insecure public Wi-fi network

3 **LONG AND STRONG** use stong, complex passwords; never use social media passwords for business accounts

4 **WHEN IN DOUBT, CAST IT OUT** delete suspicious emails, texts or online posts

5 **SEE SOMETHING, SAY SOMETHING:** report any suspicious behavior in the workplace or unusual emails and attachments to IT, Security or your manager

6 **Report stolen finances or identities and other cyber crimes** to the Internet Crime Complaint Center www.isee3.gov and local law enforcement

**Figure 3.6:** Cyber security practices for event organizers

## The convergence of cybersecurity within the event industry's digital ecosystem

Securing event ICT ecosystems in the future, where thousands of mobile devices connect to onsite wireless access points and dedicated Wi-Fi networks for cashless point of sales transactions, ticketing, social media and event information, remains a daunting task for event IT security teams (Lakhani, 2019). Moreover, this challenge will be further exacerbated through the COVID-19 global risk shock and the pivot from traditional office workplaces to the 'new normal' of tele-working from home-based workplaces and the emerging fourth industrial revolution, Industry 4.0; characterized by the integration of physical and computational elements and the emergence of cyber-physical technologies, such as the internet of things (IoT) and radio-frequency identification (Lal, 2020; US Cybersecurity and Infrastructure Security Agency, 2020; Xu et al., 2018).

## Shaping the response to future cyber threats

What is the role of the public and private security sectors for shaping and influencing best responses to future cyber threats to the events industry sector? First, IT security professionals should seek to better understand the challenges confronting event organizers for the implementation of industry cyber security best practices, for example: resourcing and budget constraints; the lack of dedicated staff with an IT security focus; lack of cyber risk awareness and the severity of consequences from a cyber incident; lack of business continuity preparedness and organizational resilience to cyber-incidents and ICT system failures; appreciate that implementing complex cybersecurity policies practices and protocols are likely to have negatively impact on workplace productivity and less likely to be implemented (Cavelly, 2014; Kirlappos et al., 2014; Payne et al., 2019). Second, taking steps to improve the cybercrime evidence base through consistent use of language and methodologies for the collection and measurement of cybercrime data, encourage reporting of cybercrime in the workplace through cybersecurity awareness and training. Third, seek opportunities to strengthen domestic legislative frameworks and the harmonization of cybercrime legislation *between* transnational jurisdictions to increase the risk of prosecution for would-be cybercriminals and raise the cost of 'doing business' for cybercriminals (Stratton et al., 2017). Fourth, actively promote a culture of collaboration and digital trust within the events industry ecosystem through the public and private security sector industry to enhance access to timely cybersecurity and threat information.

Cybercrimes are a complex problem, global in nature and remain a persistent and serious threat to the organizers and their events. As the physical world and virtual space becomes increasingly integrated, ICT systems, networks and data will continue to remain vulnerable to existential cyber threats from sophisticated cyber-criminals and other malicious actors who possess the intent and capability to exploit vulnerabilities to steal data, commit fraud and disrupt access to data within the events digital ecosystems. To meet this challenge, event organizers supported by the public and private security sector partners must continue to converge and adapt their cyber-security defenses to meet these future cyber-threats. The ongoing convergence of the public and private security sectors, collective security initiatives for the provision of industry leading advice on cost effective, 'best of breed' cybersecurity tools and the availability of government sponsored cybersecurity training will significantly enhance the events industry resilience to cyber-incidents, malicious or accidental.

Cybercriminals are agile, adapt and continuously evolve their tactics, techniques, and technologies to target and exploit the events industry ICT systems whose cyber-defenses are known to be far more vulnerable and less sophisticated than larger organizations. While it has been noted that the events industry sector workplace is constrained by limited resources, workplace cybersecurity training and cybercrime situational awareness remain fundamental building blocks for effective information security and the prevention of cybercrime within the industry.

# Conclusion

This chapter explored contemporary insights into event risk management and how event organizers approach risk-based decision-making in today's volatile, ambiguous, complex and uncertain world. The inter-related risk constructs pertaining to socio-cultural theoretical perspectives of risk were explored to provide insights into how event organizers perception of risk influences their approach to risk management, be it subjective or objective. It was concluded, that while event organizers rely on intuitive risk judgments based on a foundation of experience which seldom incudes direct experience with the risk event, this should not be considered erroneous or overly biased, as compared to probabilistic risk assessments. Following on, it was surmised that event organizers rarely have the necessary information and time to apply analytical based, decision-making processes but rather they relied on naturalistic decision-making (heuristics); leveraging their expertise, experience and intuition to reach timely and 'satisficing' decisions. Notwithstanding, it was noted that an event organizer's decision-making could be improved through adopting repeatable and systematic, decision-making models, such as the OODA loop.

The second part of the chapter considered two low probability, severe impact risks, domestic terrorism and cyber-criminals attacks. While events will continue to remain attractive targets for various terrorism threat actors into the foreseeable future, it is possible for event organizers to reduce the risk of a terrorist attacks through applying SCP counter terrorism solutions that are cost-effective, feasible and offer opportunities for enhancing an event team's resilience and capability to respond and recover from critical incidents. The rapid onset of the digital age has created unprecedented opportunities for increasingly, sophisticated, and capable cyber-criminals and cyber-deviant entrepreneurs to target event organizers whose vulnerable cyber-defenses are known to offer low risk, high return criminal opportunities. Cybercrimes will continue to remain a persistent and serious threat. Event organizers in collaboration with their public and private security sector partners must continue to converge and adapt their cyber-security defenses to meet these future cyber-threats.

The awareness and maturity of risk management within the events industry is undeniably growing as event managers migrate from an insurance-led approach to an event management led approach. However, it remains evident that the events industry faces ongoing challenges in developing a mature level of capability to proactively manage event risks; be it a subjective, risk ranking approach or more quantitatively, through probability risk assessments. As an industry, it is essential to pursue further academic research into event risk management and to provide opportunities for professional development of the next generation of events leaders in risk management.

## References

Anarumo, M. (2011) The practitioner's view of the terrorist threat, in Kennedy, L., & McGarrell, E. (eds) *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice.* pp. 56-89.

Andress, J. (Ed.) (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. London: Elsevier.

Ash, J., & Smallman, C. (2010). A case study of decision making in emergencies. *Risk Management*, *12*(3), 185-207.

Ashwin, P., & Wilson, M. (2020) *Event Industry Preparedness and Resilience Survey.* https://www.blerter.com/lp/event-preparedness-resilience-survey-report.

Australian Cyber Security Centre. (2020) *Cyber Security and Australian Small Businesses Survey Results.* https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf (Accessed: 22 August 2020).

Aven, T., & Renn, O. (2009) The role of quantitative risk assessments of characterizing risk and uncertainty and delineating appropriate risk management options with special emphasis on terrorism risk, *Risk Analysis, 29* (4), pp. 587- 600.

Beck, U. (1999) *World Risk Society.* Cambridge: Polity Press.

Beck, U. (2006). Living in the world risk society. *Economy and Society*, *35*(3), 329-345.

Berlonghi, A. (1990) *The Special Event Risk Management Manual.* Dayton, CA: Bookmasters Inc.

Bjorgo, T., & Silke, A. (2019). Root causes of terrorism. In A. Silke (Ed.) *Routledge Handbook of Terrorism and Counterterrorism* (pp.57-65). New York: Routledge.

Boba, R. (2009) 'EVIL DONE', in Freilich, J. and Newman, G. (eds). *Reducing Terrorism through Situational Crime Prevention.* pp.71-91, Monsey, NY: Criminal Justice Press.

Bouhana, N., Malthaner, S., Schuurman., Lindekilde, L., Thornton, A., & Gill, P. (2019) Lone actor terrorism: Radicalization, attack planning and execution, in Silke, A. (ed.) *Routledge Handbook of Terrorism and Counterterrorism.* New York: Routledge, pp.112-121.

Boyd, J. (1979). New Conception for Air-to-Air Combat. (Unpublished paper). Available at: http://dnipogo.org/john-r-boyd/.

Cavelty, M. (2014) Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities, *Science, & Engineering Ethics, 20*(3), 701–715.

Chang, L., & Graboksy, P. (2014) Cybercrime and establishing a secure cyber world, in Gill, M. (ed) *The Handbook of Security.* 2nd edn. Basingstoke: Palgrave MacMillian, pp.331-339.

Clark, J., & Saviour, S. (2018) *Negligence: What is Reasonably Foreseeable.* https://stewartmckelvey.com/thought-leadership/client-update-negligence-what-is-reasonably-foreseeable, (Accessed:15 December 2020).

Clarke, R., & Newman, G. (2006) *Outsmarting the Terrorists.* Westport, Connecticut: Praeger Security International.

Department for Digital, Culture, Media and Sport. (2019) *Cyber Security Breaches Survey 2019.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/ (Accessed: 12 August 2020).

Ellis, R., Fabtz, A., Karimi,F., & McLaughlin, E. (2016) *Orlando Shooting: 49 Killed, Shooter Pledged ISIS Allegiance.* Orlando shooting: 49 killed, shooter pledged ISIS allegiance (cnn.com) (Accessed: 1 December 2020).

Ezell, B., Bennett, S., Von Winterfelt, D., Sokolowki, J., & Collins, A. (2010) Probabilistic risk analysis and terrorism risk, *Risk Analysis*, *30* (4), 575-589.

Ferrara, D. (2020) *Judge Approves $800 million Settlement for Route 91 Victims.* https://www.reviewjournal.com/crime/courts/judge-approves-800m-settlement-for-route-91-victims-2133490/ (Accessed:15 December 2020).

Freilich, J., Chermak, S., & Hsu, H. (2019) Deterring and preventing terrorism, in Silke, A. (ed.) *Routledge Handbook of Terrorism and Counterterrorism.* New York: Routledge, pp. 434-443.

Furnell, S., Emm, D., & Papadaki, M. (2015) The challenge of measuring cyber-dependent crimes, *Computer Fraud, & Security, 10*, 5-12.

Getz, D. (1997) *Event Management and Event Tourism.* New York: Cognizant.

Goldblatt, J, Dr. (2011). *Special Events: A New Generation and the Next Frontier.* 6th edn. New Jersey: John Wiley, & Sons Inc.

Gordon, S., & Ford, R. (2006) On the definition and classification of cybercrime, *Journal of Computer Virology, 2,* 13-20.

Haberfeld, M., & von Hassell, A. (2011). Proper proactive training to terrorist presence and operations in friendly urban environment. In M. Haberfeld, & A. von Hassell (Eds.), *A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned* (pp. 9-22). New York: Springer.

Hackread. (2017) *Coachella Festival Website Hacked; User Data at Risk.* https://www.hackread.com/coachella-festival-website-hacked-user-data-at-risk/ (Accessed: 15 August 2020).

Hall, S., Manning, D., Keiper, M., Jenny, S., & Allen, B. (2019). Stakeholders perception of critical risks and challenges hosting marathon events: An exploratory study. *Journal of Contemporary Athletics, 13*(1), 11-22.

Hesterman, J. (2015) *Soft Target Hardening: Protecting People from Attack.* Boca Raton, FL: CRC Press.

Hillson, D. (2016) *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk*. London: Kogan Page Ltd.

Hinduja, S., & Kooi, B. (2013) Curtailing cyber and information security vulnerabilities through situation crime prevention', *Security Journal*, *26*(4), 383-402.

Hopkin, P. (2010). *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management* (2nd edn). London: Kogan Page.

IBM Security and Ponemon Institute (2020). *Cost of a Data Breach Report 2020.* New York: IBM Security.

International Organization for Standards. (2018). *ISO 31000: Risk Management – Guidelines*. 2nd ed. Zurich: International Organisation for Standards (ISO).

Khir, M.M. (2014). *Developing an Event Safety Typology: A Qualitative Study of Risk Perception amongst Event Planners and Venue Managers in Malaysia*. PHD Thesis. Liverpool John Moores University. Available at: http://researchonline.ljmu.ac.uk/id/eprint/4441/1/157529_2014masrurphd.pdf.

Kirlappos,I., Parkin, S., & Sasse, A. (2014). Learning from Shadow Security: Why understanding non-compliant behaviors provides the basis for effective security. Available at: https://discovery.ucl.ac.uk/id/eprint/1424472/1/Kirlappos%20et%20al.%20-%202014%20-%20Learning%20from%20%E2%80%9CShadow%20Security%E2%80%9D%20Why%20understanding.pdf.

Klein, G. (1993). A Recognition-Primed Decision (RPD) Model of Rapid Decision Making. In G. Klein, J. Ornaanu, R. Calderwood, & C. Zsambok (Eds.), *Decision Making in Action: Models and Methods* (pp. 138-147). Norwood, NJ: Ablex Publishing Corp.

Klein, G. (2008). Naturalistic decision making. *Human Factors: The Journal of Human Factors and Ergonomic Society*, *50*(3), 456-460. Available from: https://journals-sagepub-com.ezproxy4.lib.le.ac.uk/doi/pdf/10.1518/001872008X288385.

Lakhani, A. (2019) *Ensuring Cybersecurity at Big Events this Summer*. https://www.fortinet.com/blog/business-and-technology/cybersecurity-big-summer-events (Accessed at: 26 August 2020).

Lal, A. (2020) *Building Cyber Resilience Post COVID-19 19.* https://www.cpomagazine.com/cyber-security/building-cyber-resilience-post-covid-19/ (Accessed: 28 August 2020).

Laybourn, P. (2003) Risk and decision making in events management, in Yeoman, I. (ed). *Festival and Events Management: An International Arts and Culture Perspective.* New York: Routledge.

Levi, M., Doig, A., & Gundur, R. (2017) Cyberfraud and the implications for effective risk-based responses: Themes from UK research, *Crime Law Society Change, 67*, 77–96.

Lupton, D. (2013). *Risk.* 2nd edn. New York: Routledge.

McGuire, M., & Dowling, S. (2013) Cybercrime: A review of the evidence, *Home Office Research Report 75*. London: Home Office Science.

Mcllhatton, D., Allen, A., Chapman, D., Monaghan, R., Ouillon, S., & Bergonzoli,,K. (2019). Current considerations of counter terrorism in the risk management profession. *Journal of Applied Security Research*, *14*(3), 350-368.

Mercury News (2020). *Coachella Festival Website Hacked, Users Personal Data Stolen.* https://www.mercurynews.com/2017/03/01/coachella-festival-website-hacked-users-personal-data-stolen/ (Accessed: 20 August 2020).

Millaire, P. Sathe, A., & Thielen, P. (2017) *What all Cyber Criminal Know: Small and Midsize Businesses with Little or No Cybersecurity are Ideal Targets.* https://www.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf (Accessed: 21 August 2020).

Ostrom, L., & Wilhelmsen, C. (2012). *Risk Assessment: Tools, Techniques and their Application*. New York: John Wiley, & Sons Inc.

Payne, B., David C. May, D., & Hadzhidimova, L. (2019) America's most wanted criminals: Comparing cybercriminals and traditional criminals, *Criminal Justice Studies*, 32(1), 1-15.

Piekarz, M., Jenkins, I., & Mills, P. (2015) *Risk and Safety Management in the Leisure, Events, Tourism and Sports Industries.* Oxfordshire: CAB International Inc.

Plous, S. (1993). *The Psychology of Judgment and Decision Making*. NY: Mcgraw-Hill Book Company.

Reason, J. (1990). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London. Series B, Biological Science*s, *327*(1241), 475–484. doi:10.1098/rstb.1990.0090.

Reason, J. (1997). *Managing the Risk of Organizational Accidents*. Surrey, UK: Ashgate Publishing Ltd.

Reid, S., & Ritchie, B. (2011) Risk management: Event managers' attitudes, beliefs and perceived constraints, *Event Management*,*15*, 329-341.

Robson, L. (2009) *Perceptions of Risk at Meetings and Conferences: An Event Planners Perspective.* PHD Thesis. University of Waterloo. https://uwspace.uwaterloo.ca/bitstream/handle/10012/4509/Robson_Linda.pdf.

Rogers, G. (1997) The dynamics of risk perception: How does perceived risk respond to risk events? *Risk Analysis*,*17*(6), 745 – 757.

Rule, J. (2013) *A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought.* Master of Strategic Studies, Dissertation. United States War College. https://www.scrummaster.dk/lib/AgileLeanLibrary/Topics/OODALoop/OODAASymbioticRelationship.pdf.

Rutherford Silvers, J. (2008) *Risk Management for Meetings and Events*. Oxford: Butterworth- Heinemann.

Slovic, P. (2000) *The Perception of Risk.* London: Earthscan Publications Ltd.

Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science*, *15*(6), 322-325.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'Digital Criminology'?. *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17-33.

Talbot, J. (2011) .What Right with Risk Matrices? Available at: https://31000risk.wordpress.com/article/what-s-right-with-risk-matrices-3dksezemjiq54-4/

Tarlow, P. (2002) *Event Risk Management and Safety*. New York: John Wiley, & Sons Inc.

UK Centre for the Protection of National Infrastructure. (2020) *Recognizing Terrorist Threats Guide.* https://www.cpni.gov.uk/recognising-terrorist-threats-guide-0 (Accessed: 10 December 2020).

UK Federation of Small Businesses (2016). *Cyber Resilience: How to Protect Small Firms in the Digital Economy*. Available at: https://www.fsb.org.uk/resources-page/small-businesses-bearing-the-brunt-of-cyber-crime.html.

US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2011). *Risk Management Fundamentals*. Available at: https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2019) C*ISA Cyber Essentials.* https://www.cisa.gov/publication/cisa-cyber-essentials (Accessed: 22 July 2020).

US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2020) *COVID-19 Exploited by Malicious Cyber Actors.* https://us-cert.cisa.gov/ncas/alerts/aa20-099a (Accessed: 22 August 2020)

US Department of Homeland Security. (2020) *Homeland Threat Assessment.* https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf (Accessed: 30 November 2020).

US National Counterterrorism Center. (2020) *Counter Terrorism Guide for Public Safety Personnel.* https://www.dni.gov/nctc/jcat/index.html (Accessed: 20 November 2020).

Verizon. (2020) *2020 Data Breach Investigations Report.* https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (Accessed: 13 August 2020).

Wall, D. (2001) Cybercrimes and the Internet, in Wall, D (ed) *Crime and the Internet.* New York: Springer.

Whitman, M., & Mattord, H. (2005) *Principles of Information Security*, 2nd edn. Boston: Thompson Course Technology.

Willis, H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis*, *27*(3), 597-606.

Xu, L., Xu, E., & Li, L. (2018) Industry 4.0: State of the art and future trends, *International Journal of Production Research*, 56(8), 2941-2962.