CONVENTION CENTRE SECURITY

AIPC

EXCELLENCE IN CONVENTION CENTRE MANAGEMENT

Good Practice Managing Critical Threats

In a world in which convention centres face constant change on a number of fronts, no challenges are as important as those effecting the safety and well-being of staff, clients and the public.

AIPC
EXCELLENCE IN CONVENTION CENTRE MANAGEMENT

With the global spread of incidents and the diversification of threats, security is now a primary concern and source of convention centre client expectations everywhere in the world. As both beneficiaries of good security-related practices and a primary source of the expertise and related experiences needed to create them, AIPC members have a key role in their development – and this was the purpose behind the creation of the AIPC Security Best Practices Task Force in November 2018 that has resulted in this document.

It will now form part of the complement of AIPC Management Tools that includes a range of practical, industry-specific initiatives under the overall umbrella of the AIPC Quality Standards program and is available to all AIPC member centres for their adoption, adaptation and / or consideration as they develop and maintain their own centre-specific policies and practices. It will also evolve as more information becomes available in this critical area of centre practice.

AIPC acknowledges the invaluable support and assistance provided in the course of developing these guidelines, in particular from project coordinator Glenn Schoen of Boardroom @ Crisis; Michiel Middendorf, General Manager World Forum Convention Center The Hague as the driving force behind its development and the members of the Security Task Force representing the contributions of a wide range of AIPC member centres. It is through their dedication and hard work that this valuable tool has been created for the benefit of all AIPC members.

Aloysius Arlando AIPC President

It is the hope of AIPC management that the information provided in this document can contribute to the further emergency preparedness and well-being of its membership and the global public it serves.

The Security Task Force of the International Association of Convention Centres (AIPC) created this security good practice guidance in December 2018 – May 2019 to help its members address the recent global increase in several critical security threats, notably terrorism, active assailant attacks and high-impact cybercrime threats.

These threats can be seen as critical in terms of their ability to cause swift and substantial harm to people and the key assets, processes and reputation of convention centres. Indeed, from Las Vegas to Manchester to Nairobi to Melbourne, a growing number of convention centers have suffered from significant incidents of late.

The guidance in this document is offered as a list of suggestions that might be added to the basic physical and cyber security measures convention centres already have; what some professionals are calling the “new basic”. This is thus not meant as a ‘how to’ manual on convention center security but rather a fresh compilation of newer, recently applied measures that a growing number of AIPC members are using or considering to meet critical physical and cyber threats.

Specifically, this good practice guidance aims to:

- Offer new ideas and insights and prompt fresh thinking on security measures;
- Be as practical and actionable in nature as possible;
- Be as recent as possible, most of it stemming from 2017-2019;
- Where available provide options, including cost-saving ones; and
- Be useful irrespective of the structure of the security function at a convention center (for instance whether Security is combined with Safety, or whether Physical Security and IT/Cyber Security are currently linked or not).

The information contained in this document stems in large part from the members of the AIPC Security Task Force, formed in November 2018 at the AIPC Operations Summit in Barcelona, Spain. The Task Force is comprised of security (and safety) professionals who in many cases have tried and adopted new security measures at their convention centers in recent years in response to various growing, evolving threats, and who have been willing to share their expertise with fellow AIPC members.

In addition, a number of other experts and organizations were consulted for additional information. These Task Force members and experts are:

AIPC Security Task Force

Carlos Moreno Clemente | Head of Mobility, Fira Barcelona

Rik Hoogendoorn | Manager Safety & Security, RAI Amsterdam

Darren Horne | Senior Manager Security & Safety, Melbourne Convention Exhibition Centre

Mark Laidlaw | Operations Director, Scottish Event Campus

Michiel Middendorf | General Manager, World Forum

Robert Noonan | Chief Information Security Officer, Boston Convention & Exhibition Center

Tomas von Tourtchaninoff | Head of Unit, Safety & Security, Stockholmsmassan

Muhammad Yusri | Manager Venue Security, Crime Prevention and Operations, SingEx

Other Contributors

Gerard van Duykeren | CEO, The Security Company

Godfried Hendricks | President-Elect, ASIS International

Peter O’Neil | CEO, ASIS International

Rene Polfliet | Global Security Director, Heineken

Florian Roetheli | International Events Manager, Red Bull

Glenn Schoen | CEO, Boardroom@Crisis BV

Coordination of the gathering, vetting, formatting and publishing of this information was performed by Glenn Schoen of Boardroom@Crisis BV, based in the Netherlands.

BOARDROOM@CRISIS
Enabling Preparedness

DISCLAIMER: A number of companies and products are mentioned in this document as examples of firms and tools that provide a particular capability. Their mentioning does not imply, directly or implicitly, any kind of endorsement on the part of the AIPC. They are mentioned solely as the kind of examples for security staff to consider when it comes to said types of firms or products.

How to Use This Guide

The information in this document is divided into five types of measures:

1 | Organizational Security Measures

2 | Physical Security Measures

3 | Electronic Security Measures

4 | Human-based Security Measures

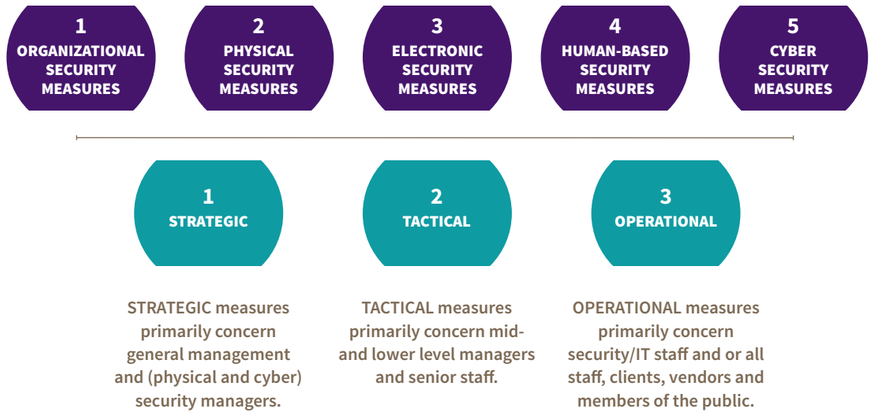
5 | Cyber Security Measures

Within these five sections, measures are grouped functionally at three levels:

1 | Strategic

2 | Tactical

3 | Operational



As not all measures can be clearly placed in one category or another, and functions and roles are sometimes hard to define, there will by necessity be some overlap between these.

As no two convention centres are the same, the advisability, applicability and proportionality of measures in terms of size, scale, function and environment should be taken into account when considering their use.

Where documents or other resources are mentioned in the text, these should, in most cases, be retrievable via the link provided or by using an Internet search. A (very few) documents mentioned are restricted, and may require direct contact with the owner entity to obtain.

1 GOOD PRACTICE: Organizational Security Measures

Strategic Level

Organizational Security Measures

1 | To limit the risk of ineffectiveness and inefficiency in security planning, ensure that the entire security program of your convention center:

- Is based on assessed threat vulnerabilities and risks;
- Aligns with your site's safety program;
- Aligns with your organization's core business objectives;
- Incorporates controls to meet applicable data privacy regulations; and
- Counts both effectiveness and efficiency as core values, so that security measures not only mitigate risks appropriately but are sustainable over time.

2 | To help govern, structure, manage, improve, review and demonstrate the quality of your convention center security, adopt national and or international standards and or guidelines. Among international standards and or guidelines to consider are (separate standards expressly for cyber security are listed in the Cyber Security Measures section):

- ISO 31000 Risk Management
- ISO 27001 Information Security
- ISO 22301 Business Continuity
- EU CEN/TS 17091 Crisis Management as a Strategic Capability
- American ANSI ASIS International CSO-1 Security Leadership
- ISO 45001 Occupational Health & Safety Management Systems (for links between Security and Safety)
- International Association of Venue Managers "Convention Center Security Guidelines". Note: Considered comprehensive and exhaustive, this well-regarded widely used guidance document is foremost focused on baseline security. (August 2017)
- UK National Arenas Association (NAA) Safety Advisory Group "A - Guide". Note: This is a practical, detailed, alphabetical good practice guidance document issued in March 2016 focused on event safety that includes a wide range of security practices.

3 | To manage the security function as optimally as possible and work towards operationalizing the evolving new global Enterprise Security Risk Management (ESRM) framework, consider use of a dedicated security management software platform. In many convention centers, IT departments already use a form of cyber security management platform but relatively few use one for physical operations, or one that uses the ESRM approach and combines the two in a single approach.

4 | To improve convention centre security managers' ability to more rapidly reduce key risks in general, save costs, and improve emergency situation performance, foster their connectivity to international platforms of industry colleagues, security learning and security expertise. A large number of countries have local, regional and national networking platforms to this effect, and there are several international ones as well. Notable among these are ASIS International (the 36,000+ member leading global security professionals' networking, learning and training organization), and the US State Department's Overseas Security Advisory Council or OSAC, with well over 100 chapters worldwide. While the latter is a US-government supported network, leadership of most convention centres – who worldwide serve US clients – can join, and many are members.

5 | To keep abreast of threats and potential security weaknesses and be able to assess, share, monitor and prepare to address these threats, perform regular security threat and risk assessments for the facility as a whole, and per event. Ensure that assessments (or evaluations) match safety and (other) IT/cyber plans, and include considerations of the specific audience/participants of the event.

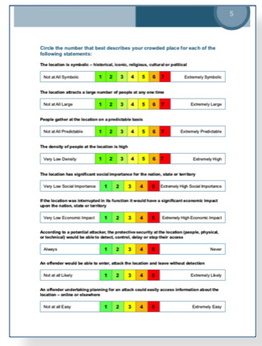
As an example of good practice, SingEx in Singapore maintains its own proprietary 'Security Planning Guide for Event Organizers' which has been vetted by police and has separate sections for assessing risk based on:

- Nature of the event
- Location of the event
- Attendees of the event
- High-lights of the event
- Attacker perspective | timing and event segments
- Attacker perspective | vulnerabilities from start to finish of event

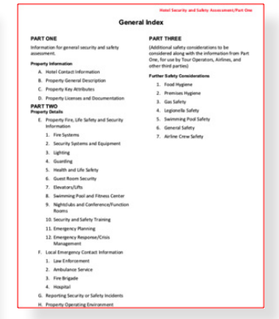
For guidance on conducting threat and risk assessments geared towards critical threats (notably terrorism and active assailants), see:

- Australia-New Zealand Counter Terrorism Committee (ANZCTC) "Crowded Places Self-Assessment Tool" (2018)

www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/crowded-places-self-assessment-tool.pdf



6 | To assess security (and safety) threats and control measures against and at hotels that are part of a convention centre, see the US State Department Overseas Security Advisory Council (OSAC) Hotel Security Working Group "Hotel Security and Safety Assessment Form" (Version 2014, Updated).



7 | To assess individuals who might be prone to radicalization and violence and present a threat, see: Monica Lloyd, UK CREST and the Economic and Social Research Council (ESRC), "Assessing the Risk of Extremist Violence" (2019): crestresearch.ac.uk/resources/extremism-risk-assessment-directory/

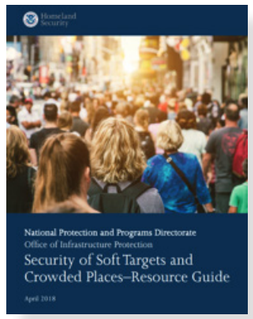
This includes guidance on:

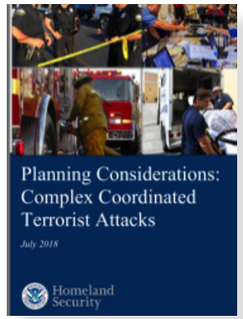
- Extremism Risk Guidance (ERG22+)
- Identifying Vulnerable People (IVP)
- Multi-level Guidelines (MLG Version 2)
- Terrorist Radicalization Assessment Protocol (TRAP-18)
- Violent Extremism Risk Assessment Version 2 Revised (VERA-2R)

8 | To help update threat and risk assessments and leverage this for emergency planning and general preparedness, ensure good connectivity with local law enforcement, government security agencies, local, regional and national security platforms / associations / organizations, and subject matter experts. Regard subject matter experts as a separate, valued category of information as they track particular threats and their changes over time, both in the physical and cyber domains, and can often note and comment on this openly, without government confidential information restrictions.

9 | To properly plan for and manage (extreme) emergencies effectively, prepare a contingency plan and test and exercise its core components once ready. The plan should cover the widest range of incidents and be integrated with safety plans. Place emphasis on being able to manage emergencies during events and their separate stages. The six event stages many security experts discern for contingency plans are: arrival, assembly, ingress, event (or experience), egress and dispersal. For guidance on preparing a contingency response plan, see:

- UK NACTSO “Crowded Places Guidance”
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf
- Singapore Police: “Contingency Planning and Protective Security Advisories”
- Singapore SGSecure “Guide for Workplaces”
- Australia AS 3745/2010 “Planning for Emergencies in Facilities”
- US Department of Homeland Security (DHS) 2018 “Soft Targets and Crowded Spaces – A Resource Guide”
www.dhs.gov/sites/default/files/publications/Soft_Targets_Crowded%20Places_Resource_Guide_042018_508.pdf
- While designed as guidance for first responders, the US Federal Emergency Management Agency (FEMA) guidance “Planning Considerations –Complex Coordinated Terrorist Attacks” offers insight on all of the stakeholders that convention centres might have to deal with in the aftermath of an incident.
www.fema.gov/media-library-data/1532550673102-c4846f270150682decbda99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf
- Similarly, guidance from the DHS Center of Excellence CCICADA at Rutgers University offers detailed insight on a range of contingency plan aspects.
https://ccicada.org/wp-content/uploads/2017/05/Best-Practices-Anti-Terrorism-Security-Resource-Guide.pdf





10 | To manage sudden increases in the local threat environment, including a direct threat against the convention center, develop and maintain a threat and security measure escalation plan as part of your contingency plan. Where possible, align the plan with existing government threat escalation plans. Among measures to consider:

- Increasing the security posture of a facility by deploying more guards or augmenting the unarmed guard force with armed guards, or police.
- Increasing security access control and screening procedures, e.g. by doing ID checks, checking all bags being carried inside, deploying hand-held metal detectors, or decreasing the number of authorized access points.
- Temporarily stopping the flow of mail or relocating the mail room to a remote site or location (particularly if there is a possible threat of suspicious items being sent by mail).
- Placing one or more security officers on duty in the security control room, so that more alarms and camera images can be monitored live;
- Having a way to inform people about a development rapidly, e.g. via text messages, email, a messenger service /event App or other communication means. For example: “There has been a security incident at the nearby train station. As a general precaution to protect our premises, we will shortly be increasing our security measures. If you see anything suspicious, please report this to a security officer right away.”
- Having a way to alert and or instruct people on the premises about an acute threat. Options might include an audible alarm signal, use of a voice broadcast system, use of a mass text message system, use of a mass email system, or use of a messenger service like a WhatsApp group. It is generally considered good practice to:

  > Accompany an alert message with a short instruction, if possible.

  > Repeat the alert message.

  > Issue the alert message in multiple languages, if possible (depending on the people / event attendees on the premises).

- For guidance and suggestions on specific security measures to undertake under different security threat levels, see:

  > Appendix 2 of the Australian National Guidelines on Protection of Critical Infrastructure from Terrorism:
www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

  and see

  > UK National Counter Terrorism Security Office – NSM National Stakeholder Menu of Tactical Options – Level 5 “Critical” (2018). See Appendix 2

  > UK National Counter Terrorism Security Office – Graduated Security Plan (GraSP) (2018). See Appendix 3

11 | To ensure that your threat and security measure escalation plan works and can be executed in a real emergency, test it at least once a year, if only in ‘walk-through’ fashion if a live test is not possible.

12 | To check whether the security measures taken to protect your convention center are effective and cover all the (latest) threats identified, perform security audits on a regular basis. Perform at the very minimum one a year for the entire facility. To augment larger audits, perform regular spot checks and reviews of security staff and physical, electronic and IT measure performance/status. Capture, study, share and use the results to drive improvements. For guidance on conducting security audits, see:

- ANZCTC Crowded Places Security Audit –
www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/crowded-places-security-audit.pdf

13 | To improve the police response in any future incident at your convention centre, consider offering or providing police:

- Regular orientation visits to and walk-throughs of the facility.
- Detailed floor plans and the Security Plan of the facility.
- Allowing police special forces to train at the facility during off-hours.
- Allowing police representatives to attend crisis management exercises at the facility.

14 | To manage major emergencies, be they of a security, safety, IT, public relations, integrity or other nature, set up, equip, train and maintain a convention center Crisis Management Team (CMT). Have the CMT develop and train on scenarios starting with the leading safety, security and IT risks identified in risk assessments and audits. Good practice as tested at the World Forum in The Hague, The Netherlands ensures that the CMT has the use of a fully furnished CMT Crisis Room, that senior management is directly involved with the team and that as part of the team, the Security Manager has enough autonomy to handle a security crisis situation in the absence of availability or time on the part of the senior most venue manager. For guidance on requirements for setting up and operating a Crisis Management Team, see:

- ISO 22301 Business Continuity
- EU CEN/TS 17091 Crisis Management as a Strategic Capability

As examples of crisis management notification, reporting, communications, coordinating and task tracking software that management can use, see for instance the software developed by: Fact24 (F24), Everbridge, Amika, Send Word Now, Evernote, Merlin Software CrisisSuite, Onsolve, and Clearview.

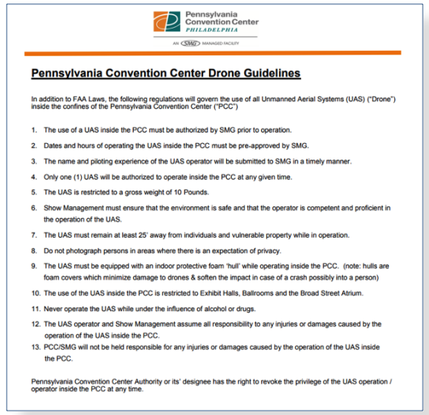
15 | To help prepare for major emergencies, have the Crisis Management Team, security department and safety officials conduct exercises that (at least) focus on:

- Dealing with a major violent incident.
- Dealing with a major cyber attack.
- Dealing with a loss in phone and IT services.
- Dealing with a complete loss of power.
- Restoring critical building services.
- Registering and tracking victims wounded in an incident.
- Providing psychological care for traumatized staff.
- Securing evidence to help authorities with the investigative process.

A practical standard for conducting exercises is that of the German Office for Federal Protection and Disaster Assistance “Guideline for Strategic Crisis Management Exercises.” (2011)

16 | To manage the threat of unauthorized use of drones outside and inside your convention center, consider developing a policy that limits, prohibits or otherwise restricts the use of drones. Check if this can be supported by local law, and seek to publicize these restrictions so clients and the public are aware they will break policy (if not local ordinances / the law) and may face consequences if they do this anyway.

An example of (counter) drone use policy guidance from the Pennsylvania Convention Center in Philadelphia is available online at:
www.paconvention.com/assets/doc/Plan-of-Ops-Final-Revised-February-2017-53e23a7749.pdf



Pennsylvania Convention Center PHILADELPHIA
AN SMG MANAGED FACILITY

Pennsylvania Convention Center Drone Guidelines

In addition to FAA Laws, the following regulations will govern the use of all Unmanned Aerial Systems (UAS) (“Drone”) inside the confines of the Pennsylvania Convention Center (“PCC”)

1. The use of a UAS inside the PCC must be authorized by SMG prior to operation.
2. Dates and hours of operating the UAS inside the PCC must be pre-approved by SMG.
3. The name and piloting experience of the UAS operator will be submitted to SMG in a timely manner.
4. Only one (1) UAS will be authorized to operate inside the PCC at any given time.
5. The UAS is restricted to a gross weight of 10 Pounds.
6. Show Management must ensure that the environment is safe and that the operator is competent and proficient in the operation of the UAS.
7. The UAS must remain at least 25’ away from individuals and vulnerable property while in operation.
8. Do not photograph persons in areas where there is an expectation of privacy.
9. The UAS must be equipped with an indoor protective foam ‘hull’ while operating inside the PCC. (note: hulls are foam covers which minimize damage to drones & soften the impact in case of a crash possibly into a person)
10. The use of the UAS inside the PCC is restricted to Exhibit Halls, Ballrooms and the Broad Street Atrium.
11. Never operate the UAS while under the influence of alcohol or drugs.
12. The UAS operator and Show Management assume all responsibility to any injuries or damages caused by the operation of the UAS inside the PCC.
13. PCC/SMG will not be held responsible for any injuries or damages caused by the operation of the UAS inside the PCC.

Pennsylvania Convention Center Authority or its’ designee has the right to revoke the privilege of the UAS operation / operator inside the PCC at any time.

17 | To assist clients in making their own event security preparations and reducing your own convention center organization’s workload, consider developing a (suggested) event safety and security standard for clients to use and apply. A growing number of leading companies who use convention centers already have such an ‘own’ standard. An example of a good practice is the (restricted) Heineken Event Standard which includes security operations sections on everything from access control to emergency planning. The company security team deliberates with convention centre security staff where an event is due to take place well in advance, and collaborates closely throughout implementation.

Example of sections of the Heineken Security Standard:

Under policy document HeiRule 25: Physical Security – Heineken Event Standards: Required: Event Security, Safety & Health (ESSH) Plan to include:

1. Risk Assessment
2. Venue Security Measures
3. Access Control Measures
4. Operational Security Procedures
5. House Rules
6. Alcohol & Minors Policy
7. Safety & Health Measures
8. As applicable, Transportation Measures
9. (Planning Matrix – List of Other Relevant Matters)

18 | To brief appropriate external parties (who might be allowed to see restricted/confidential information) like client security managers, client executive protection teams, and police officers, make a briefing package such as on PowerPoint that can be used to visually inform them of the structure and main operations of the security department. Such a briefing not only has immediate high security value in terms of explaining how things work, what assets are available and where external parties ‘fit’ in the security plan, but can also be seen as a value-add for the sales and marketing department in that it demonstrates the capabilities, quality, preparedness and professionalism of the security department.

The following few slides are part of a sample briefing deck that can also be used for external arties showing a part of the security (and safety) improvement process and risks areas being covered at the RAI Amsterdam:

Tactical Level
Organizational Security Measures

19 | To better manage the threat of explosives or other weapons being hidden at a venue prior to an event, consider:

- Having a visual search procedure security staff can perform, per room or space or zone, with a tag/sticker/room lock that can be left behind indicating the area has been searched.
- A protocol for keeping swept areas secure prior to use.
- Using explosive-detection trained dogs to perform bomb checks.
- Including non-security staff as part of the awareness plan and provide protocols for them to use.

20 | To better manage bomb threats in real-time, one of the most frequent, acute and disruptive types of threats facing convention center operations, and events in particular, have a procedure in place and train staff to follow the protocol.

For guidance on managing a bomb threat (having a plan, what to do, checklist, training video), see:

- US DHS bomb threat management materials (updated as of 2019): www.dhs.gov/what-to-do-bomb-threat
- US DHS bomb threat checklist (2017): www.dhs.gov/sites/default/files/publications/dhs-bomb-threat-checklist-2014-508.pdf
- US FBI-DHS bomb threat guidance flyer (2016): www.dhs.gov/sites/default/files/publications/dhs-doj-bomb-threat-guidance-brochure-2016-508.pdf

21 | To minimize long lines of people standing outside the convention center in unprotected areas prior to a big event, develop a plan to facilitate security screening ingress before events. A good practice pilot program run by the RAI Amsterdam in February 2019 featured use of a dedicated Crowd Control Room to follow and facilitate the flow of people from public and semi-public areas into secure interior areas during the multi-day 2019 ISE Conference attended by over 80,000 people. The successful pilot included use of extra access control entry points, screening technology, forward-deployed sensors, CCTV and staff.

22 | To assist your own and area transportation companies (bus, tram, trolley, train, taxi) serving your convention center, provide them with information on how to improve their own security, and how to contribute to the local area monitoring and 'early warning' network. For guidance on improving transportation and particularly bus security around / to convention centers, see:

- UK Department for Transport: "Bus and Coach Security Recommended Best Practice" (3rd Edition, July 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730644/bus-and-coach-security-recommended-best-practice.pdf

23 | To manage an armed attacker/armed intruder scenario, design, implement and test a so-called 'lockdown' or 'in-vacuation' procedure. Secure professional advice in doing so, paying particular attention to:

- Use of alarm systems/signals to initiate procedure.
- Use of to-standard quality locks/doors/special materials to secure specific rooms/areas/spaces.
- Instructions in card or sign form to help instruct people on what to do.
- Consideration of managing the safety of groups of VIPs present on-site.
- Coordinating the procedure's design with, and collecting input from, local law enforcement.

24 | To give early warning of potentially significant safety or security incidents that could impact convention center operations (above and beyond connectivity with local law enforcement and monitoring local news), subscribe to local government alert app services, and consider subscribing to a (private sector for-pay) automated early warning news service. Examples of private global rapid alert services are SAM Desk (Canadian) and DataMnr (USA). These, using social media analysis, can issue an alert message of significant security incidents like major accidents, disasters, and (probable) terrorist attacks within minutes of them occurring, wherever in the world, and are extensively used (even) by global news agencies to give them early warning on breaking news they may to cover.

25 | To correct shortcomings after a major incident and seek to prevent a similar event in the future, conduct an all-staff Lessons Learned session in which conclusions are drawn and written out as to what could be done to further prevent or mitigate the effects of such an event should it re-occur.

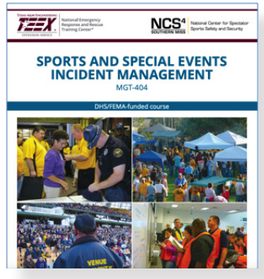
26 | To check and ensure the working status and effectiveness of all key security measures at the convention center after a major incident, conduct a near-term quick-scan security audit.

27 | As part of security evacuation and safety planning, consider whether you might want to make part of your convention center available to assist people from surrounding venues in case of a major incident there, particularly if your site includes a hotel. Among the key functions that a site can be used for in case of a major nearby incident (consider the Boston Marathon bombing in 2013) are as a:

- Safe haven for members of the public.
- Safe haven for a particular group of VIPs.
- Medical emergency First Aid and triage station.
- Support command post for First Responders.
- Location to interrogate large numbers of witnesses (by police).
- Location to collect, sort and process evidence.

Operational Level
Organizational Security Measures

28 | To properly train staff in government-professional grade event security planning, management and emergency management skills, consider allowing them to attend training courses such as those offered by government agencies, public-private organizations and private companies. Among leading instructional institutions is NCS4. An example of one of their course offerings:



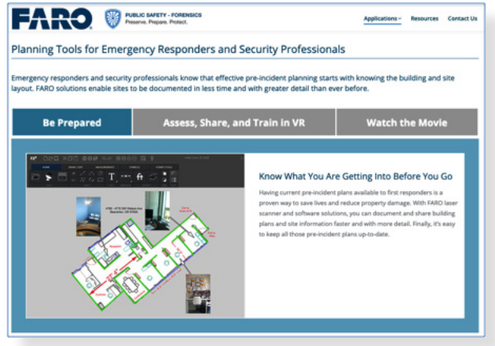
2 GOOD PRACTICE: Physical Security Measures

CAVEAT: It is noted that several of the following physical security measures contain an organizational component, meaning that planning, implementing and managing them will require the attention of organizational security measure managers.

Strategic Level
Physical Security Measures

1 | To facilitate good crisis management in an emergency, consider setting up a specially selected if not dedicated crisis room, and chose a back-up location as well. Consider further whether the crisis room might be rented out as a value-add, extra option resource for clients conducting a special event that might make availability of a crisis team room useful, like a top VIP event.

2 | To facilitate security planning for future events, and particularly physical security, consider having an interior and exterior 3D scan made of the venue and its immediate surrounding area. This could be used for large event security team planning and briefings (indicating guard stations, access routes, people flows during evacuations, emergency service deployments etc.), VIP protection (access and egress routes, counter sniper planning), drone threats and for counter-surveillance. Examples of companies that do this are FARO Public Safety & Forensics (the world's largest 3D measurement and imaging technology firm) and Japanese security firm SECOM, with extensive background in imagery for international political VIP meetings. See example image:



Tactical Level
Physical Security Measures

3 | To help protect against vehicle attacks in areas accessible by vehicles, including exterior convention center areas, parking areas, crowded/public spaces and access ramps, see the guidance provided in:

- Australia & New Zealand Counter Terrorism Committee (ANZCTC) "Hostile Vehicle Guidelines for Crowded Places" (2018): www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/hostile-vehicle-guidelines-crowded-places.pdf.

4 | To help protect against armed attacks / armed intruder / active shooter or assailant attacks (who could, of note, hide among protesters coming on site) in areas accessible by people, including crowded/public spaces, see the guidance provided in:

- Australia & New Zealand Counter Terrorism Committee (ANZCTC) "Active Armed Offender Guidelines for Crowded Places" (2018): www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/active-armed-offender-guidelines-crowded-places.pdf (and Appendices A-C).

5 | To help protect against improvised explosive device attacks in areas accessible by people, including crowded/public spaces, see the guidance provided in:

- Australia & New Zealand Counter Terrorism Committee (ANZCTC) "Improvised Explosive Device (IED) Guidelines for Crowded Spaces" (2018): www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/IED-Guidelines/IED-guidelines-crowded-places.pdf (and Appendices A-E).

6 | To help protect against so-called CBRN attacks (Chemical, Biological, Radiological, Nuclear), ensure that all critical building management system areas that need to be physically secured can and actually are secured with to-standard locks, doors, and doorframes. Further, ensure they are covered by at least two sets of electronic measures, preferably a forced entry/intruder alarm, and CCTV.

This should include access to:

- Stored food supplies.
- Water/utility pipelines.
- Air intakes/ventilation systems.

Consider, if present, these systems with regard to any VIP 'safe room' as well. For guidance, see:

- Australian National Government: www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/chemical-weapon-guidelines-crowded-places.pdf.

7 | To ensure optimal performance of your security operations center (SOC), at the next opportunity to upgrade the control room, consider:

- Whether or not it might be beneficial to relocate the SOC if it is not now in a secure area, or above ground (to guard against easy unauthorized access and against any flooding/water leak damage).
- Whether the current doors need to be replaced or reinforced to meet standards against forced entry.
- Whether or not the SOC has enough room to 'scale up' staffing in the event of a major incident, meaning there is enough room to place several additional people in the SOC in case of an emergency. This might include an extra supervisor, a police liaison officer, an extra security officer to monitor alarms and CCTV imagery live, and or an extra communications officer.
- Resilience against CBRN incidents.

8 | To be properly prepared for a CBRN (Chemical, Biological, Radiological, Nuclear) incident, discuss with specialists where, if you ever had an incident, it would be good to physically set up a (government emergency services operated) decontamination unit on the property. Would this be indoors, outdoors, does the government have a mobile decontamination tent that would be set up, and if so, where? This way you could plan for its use, were it ever necessary. More optimally, it could be test-deployed as part of an exercise on your property.

Operational Level
Physical Security Measures

9 | To act as a deterrent and to signal use of right of particular means, measures and authorities, ensure that enough and appropriate clearly visible signage is placed around the property. This should include signage indicating the presence and use of security cameras, security alarms and sensors, and signs to indicate particular items or technologies are not allowed (e.g. No Firearms, No Drugs, No Drones, No Recording Devices).

3 GOOD PRACTICE: Electronic Security Measures

CAVEAT: It is noted that several of the following electronic measures contain an organizational component, meaning that planning, implementing and managing them will require the attention of organizational security measure managers.

Strategic Level
Electronic Security Measures

1 | To prevent any improper use of electronic security measures of any kind and preclude any infringement of individual's right to privacy, do a legal check on all local and national (applicable) permit and legal requirements for use of any systems, notably CCTV and any biometric system.

Tactical Level
Electronic Security Measures

2 | Monitor the open market for potential new technologies to counter-act in- and outdoor use of unauthorized drones on, in and above convention center property. A range of companies are due to launch new technical means / tools for this purpose in the second half of 2019. In terms of currently available toolsets for meeting high-level requirements and mitigating threats emanating from drones around or in an outdoor part of a convention centre venue, consider studying the use of larger law enforcement-grade systems now in use. The few systems on the market from among others Israel, the UK, the US and Germany can under varying circumstances be hired or used in cooperation with police and, being mobile, can sometimes be pre-deployed in pilot programs. The main current technology is based on radar detection, signal detection and or interference, and triangulation of the drone pilot(s). In some cases, counter-drone tools such as shoulder-fired net launchers are part of the package. One of the systems most extensively used at top global VIP gatherings to date (2016-2019) is the Guardion system of ESG, from Germany.

3 | To properly prepare to deal with a situation in which communications shuts down due to over-use (this not infrequently happens right after a terrorist incident, when everyone tries to communicate with everyone else, taking up a lot of band-with), draw up a basic plan on what to do when this happens. Consider, among others, use of radio traffic, fixed land-line telephones, and use of messengers.

4 | To improve your convention centre CCTV system's performance for the next upgrade cycle, to the extent this is not already being done, consider adding new software/technologies that optimize a video management system's capabilities, including:

- People counter software that tracks the number of people entering and or exiting particular areas.
- Live image relay software that allows CCTV imagery to be viewed off-site by thirds parties, i.e. on an IPhone or IPad or remote station, or in the local/regional police control room (for example LiveView).
- Search software that can perform video image searches for particular persons or cars.
- Facial recognition software that can work both on an either 'black' or 'white' version application to pick out people who are in or are not in the system, i.e. recognize a particular face that is 'flagged' as a suspect person or recognize all persons that are allowed to enter a particular area.
- Gunshot detection software that can detect and pinpoint the sound of a gunshot and activate the nearest CCTV cameras and train them on that location.

5 | To prevent tailgating at entry doors into secure areas, where a person closely follows another who enters a door but without using a separate authorized access card, key, badge, or pin, consider the use of retrofit tailgate detection technology.

6 | To improve the actual screening of persons and their belongings including for explosives, ceramic knives and contraband, and improve deterrence value, consider buying or hiring body scan technology rather than metal X-ray screening technology.

7 | For mitigating the threat of so-called active assailant attacks (knife, firearm, and other weapons) through technical means, see for example the company Sound Intelligence and its audio analysis software with sensors that can be placed on CCTV that detects screams and distressed voices, and see ASIS International resources from Johnson Controls – “Gunshot Detection, Mass Notification and Critical Event Management White Paper” (2019) and “How to Complete Your Workplace Violence Plan” (2019).

Operational Level
Electronic Security Measures

8 | To enable members of the public to assist security more effectively during periods of heightened threat, consider offering members of the public visiting your convention centre a downloadable App - or giving them a web address – for people to upload smartphone images or film footage of anything suspicious, or any situation they may have witnessed requiring security’s attention (“if you see a safety or security issue, please record it and send it to us!”).

9 | To act as a deterrent, capture evidence and have an extra forward-deployed security sensor, consider - depending on the type of events you host most – having guards equipped with portable cameras. This is particularly useful for events that may see a high degree of densely concentrated crowds (concerts, dance events), possible misuse of drugs and or alcohol, or the presence of a large group of minors.

10 | Offer a ‘Safety and Security’ App for visitors to download and receive updated information on the venue layout, safety and security rules, where to get help, what to do in an emergency, where to report anything suspicious and, if possible, tie this into local government input. For instance, a number of governments including that of Japan offer free Apps with updated weather and local government warnings to advise on anything from an earthquake to a tsunami to a nuclear plant radiological release. Where possible, have the App available in different languages to accommodate foreign visitors, and consider, if available, a link to official social media channels, like the official police or emergency services Twitter account(s).

4 GOOD PRACTICE: Human-based Security Measures

CAVEAT: It is noted that several of the following human-based measures contain an organizational component, meaning that planning, implementing and managing them will require the attention of organizational measure managers.

Strategic Level
Human-based Security Measures

1 | Set up a staff security awareness program encompassing insight on different kinds of acute security threats, how to recognize signs of radicalization, how to recognize suspect situations, and how to handle during and following an incident. Include instructions for helping physically challenged persons. Use a combination of means, e.g. employee induction training, briefings, trainings, posters, flyers, online videos. Pay particular attention to extremist/terrorist threats. To help with more common challenges and prepare to have staff assist with evacuations if the need arises, also consider training staff in TIPS-type (Training for Intervention Procedures) crowd control techniques concerning:

- Assisting hysterical people;
- Assisting intoxicated people;
- Assisting people on drugs;
- Assisting people who do not speak your/the local language;
- Assisting people who are physically challenged and may need assistance during emergencies (blind, deaf, wheelchair etc.)

For personal awareness of staff (and potentially, convention center clients) on what to know and do in preparation of a possible terrorist attack, see:

- US Department of Homeland Security Infographic/poster: “If You See Something, Say Something”
  www.dhs.gov/sites/default/files/images/s4/18_0701_SeeSay_IndicatorInfographic.pd
- Singapore Police and Singapore Civil Defence Force:
  > SGSecure Flyer “Be Alert Against Terrorism”
  > SGSecure Poster “Be Prepared”
  > SGSecure App – Singapore

Examples of select awareness materials free online:

2 | To help generate executive understanding and awareness of security risks and management challenges, and to foster greater competence among managers involved in crisis management, consider conducting short, low-cost table top exercises once or twice a year. Table top exercises allow for any type of scenario to be exercised, can be done in a walk-through/talk-through or actual exercise form, tend to be high-yield on insight, and allow other stakeholders (like the police, clients, vendors, city officials) to be engaged as well.

Tactical Level

Human-based Security Measures

3 | To help realize your Duty of Care requirements towards employee travelers overseas, consider use of such international hotel review and certification companies as UGOSAFE and SafeHotels. These seek to ensure that participating hotels meet specified security and safety requirements. SafeHotels in particular is gaining significant traction in the hotel industry based on its 170+ points audits of hotels, granting three levels of certification. For details, see www.safehotels.com.

4 | To help realize your Duty of Care requirements towards employee travelers overseas, consider use of such travel briefing, tracking and alert service providers as GWS Safeture, SOS International, WorldAware (formerly IJet), Control Risks, GlobalSecure, and Riskline.

5 | Study and consider the potential use of an App meant for the public in and around your convention center by which visitors to the area could report suspicious activities directly to your security staff and or local police. Two recent programs in Spain and the UK, a mature and a pilot program, are now being monitored in other countries for local applicability.

The pilot program begun in the spring of 2019 in London, UK, uses an App called 'the Krowd.' The App allows users who see something or someone suspicious to relay messages directly to private and government security personnel in the area. The App has been developed by Krowdthink Ltd. in the UK. A similar but already matured public sector – law enforcement emergency App from Spain that convention centre staff can use to alert police to nearby dangers is the (Spanish Home Affairs Office developed) "AlertCops" App. The App, introduced in 2018 and already used in settings as large as the Pamplona 'Running of the Bulls' and MotoGP is available in several languages.

https://alertcops.ses.mir.es/mialertcops/en/index.html

Operational Level

Human-based Security Measures

6 | To improve the preparedness and deployment of security guards to manage emergencies, whether your own or contractor personnel, study and apply the guidance offered for senior and more junior managers in the new 2019 Security Guard Guideline of ASIS International.

7 | To ensure that armed security officers (if your convention centre uses these) will react effectively in extreme emergencies, make certain that the company which trains them in firearms use includes different violent attack scenarios, i.e. not just common crime but also terrorist, lone offender and scenarios involving mentally unstable individuals.

8 | Instruct staff on how to handle a suspicious object situation. For guidance, see:

- Threat Report Form Staff Can Use – Appendix B, p. 41, in UK Department for Transport: "Bus and Coach Security Recommended Best Practice" (3rd Edition, July 2018)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730644/bus-and-coach-security-recommended-best-practice.pdf

9 | Instruct staff on what to do during an emergency incident. For personal awareness of staff (and potential convention center clients) on what to do during a possible terrorist attack or other (non cyber) emergency incident, see:

- UK NACTSO – Counter Terrorism Policing Poster: "In the rare event of a firearms or weapons attack – Run Hide Tell Leaflet"

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/595437/RHT_A5.pdf

- UK NACTSO – Counter Terrorism Policing Film: "Stay Safe: Firearms and Weapons Attack"

https://www.gov.uk/government/publications/stay-safe-film

- Singapore Police and Singapore Civil Defence Force: SGSecure Poster "Guide for Workplace"
- For security staff training on what to do in an active shooter situation, see for example courses offered by the US FEMA (IS-907 online training - "Active Shooter: What You Can Do") and the US Advanced Law Enforcement Rapid Response Training (ALERRT) Center, which also serves non-law enforcement in the "Civilian Response to Active Shooter Events" (CRASE) methodology. This organization is certified by the US FBI as the (US) national standard in active shooter response training. Other methodologies taught by a variety of other institutions not certified by the FBI as a national standard but nevertheless widely used include "Run Hide Fight," "Run Hide Tell" and "Alert, Lockdown, Inform, Counter, Evacuate" (ALICE).
- HOT Protocol for what to do when encountering suspicious objects, Appendix D, p. 49, in UK Department for Transport: "Bus and Coach Security Recommended Best Practice" (3rd Edition, July 2018, 68 pages)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730644/bus-and-coach-security-recommended-best-practice.pdf

18 July 2017 — Guidance
Stay Safe Film

8 June 2017 — Guidance
Crowded places guidance

10 | Instruct staff on what to do after an emergency incident. For personal awareness of staff (and potential convention center clients) on what to know and do in the aftermath of a terrorist attack, see:

- Singapore Police and Singapore Civil Defence Force SGSecure Poster "After a Terrorist Attack"

11 | To promote awareness among vehicle operators (bus, truck, van used for convention centre business) about vehicle security and misuse of vehicles for terrorist/extremist attacks, see:

- Australian Government: Security Guidance for Truck Drivers and Operators: It's Good for Business,

www.nationalsecurity.gov.au Securityandyourcommunity/Documents/Security-guidance-for-truck-drivers-and-operators-fact-sheet.pdf

12 | To improve the ability of security officers present at convention centre events to detect indications of potential threat early, consider offering – or requesting their company provide them – courses in behavioral analysis (or 'profiling'). This should include terrorist, lone assailant, and workplace violence study cases, and possible indications of imminent attack, i.e. behaviors associated with preparations for, or the execution of, a firearms attack, stabbing attack, suicide bomb (vest) attack, and vehicle bomb attack.

13 | Train your own security staff and other (safety) first responders in the basics of recognizing and managing possible CBRN incidents. For guidance, see:

- Australian National Government:

www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/chemical-weapon-guidelines-crowded-places.pdf

5 GOOD PRACTICE: Cyber Security Measures

CAVEAT: It is noted that several of the following cyber measures contain an organizational component, meaning that planning, implementing and managing them will require the attention of organizational security measure managers.

Strategic Level

Cyber Security Measures

1 | To protect the IT infrastructure and operations of your convention center and of that of clients using the venue, have IT staff under management guidance and approval adopt a cyber security framework and policy, and have them develop a vision and strategy to protect the infrastructure. Examples of frameworks include:

- ISO 27001 series on Information Security
- US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and NIST Risk Management Framework (RMF)
- US NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171r1.pdf

- UK IASME Governance Standard (UK) (for small to medium sized organizations)

https://iasme.co.uk/wp-content/uploads/2018/01/IASMEStandardv5.pdf

- Center for Internet Security (CIS) “Controls” Version 7

Core priority in applying the standards/guidance, as applied in good practice fashion by the Boston Convention & Exhibition Center, are to perform:

- An inventory of authorized and unauthorized devices;
- An inventory of authorized and unauthorized software;
- A review of secure configurations for hardware and software on mobile devices, laptops, workstations and servers;
- A continuous vulnerability assessment and remediation (loop); and
- A continuous exercise of controlled use of administrative privileges.

Across all of these steps, the three aspects to look at consistently are:

> Vulnerability (what makes your convention centre [IT operations] vulnerable)

> Capability (what do you need to have to address your vulnerabilities)

> Mitigations (what do need to do to address your vulnerabilities)

An example of good practice of the strategic approach to cyber security as practiced by Signature Boston / Massachusetts Convention Center Authority can be found as Appendix 2 of this report.

An example of extending cyber security good practice to vendors (offering them guidance) as practiced by the by Signature Boston / Massachusetts Convention Center Authority can be found as Appendix 3 of this report.

2 | To ensure that outside of the digital domain the physical and electronic security components of a standard are followed as well, have the physical security manager sign off on these. They should include all physical and electronic measures to protect server rooms and critical (main) IT cables.

3 | To ensure good connectivity between the physical and digital security functions, have physical security and cyber security managers conduct regular joint meetings to exchange information and insights on threats, trends, and potential concerns. The real and cyber worlds often intersect if not interact when it comes to threats, particularly when organized crime or illegal activists/extremists are preparing or executing actions, giving off indications something is pending. Among the types of convention centre events that have been targeted by cyber criminals, activists and extremists in recent years are events tied to hacking, gaming, fur, fashion, sports and recreational fishing, political parties and conventions, seafood, circuses, and show animals. Many convention centres also report being a regular target of ‘common’ cyber scammers, spammers, fraudsters and criminal ransomware actors.

4 | To ensure cyber risks are reviewed in a comprehensive manner, ensure that as part of your cyber security threat and risk assessment, a detailed inventory is drawn up of both the main known cyber attack vectors against businesses / offices / convention centres in your country and region, and potentially vulnerable Building Management System (BMS) and Security Management System (SMS) nodes at your venue. The last should include known (potential) IoT vulnerabilities. Among potential attack vectors to be considered that have effected convention centres in the past:

- Email spam messages with malware
- DDOS attack on convention center web site
- DDOS attack on website of event being held at convention center
- DDOS attack on website of organization conducting event at convention center
- Phishing attack on convention center (organization), including client files
- Phishing attack on mobile devices of attendees of event – to compromise basic account information – common tricks include offers of “extra information” on stars / celebrities / tournament players in gaming, sports, entertainment events, or an offer of “faster access” or “faster downloads”.
- Spoofing attack on WiFi network
- Attack on event registration access information

Among potentially vulnerable BMS and SMS nodes (hacking) to be considered are:

- Sliding access doors and their sensors
- Elevators and elevator doors
- Parking garage doors
- Heating system
- Water pump system
- Air conditioning system
- Refrigeration system
- Alarm system
- CCTV system
- Electronic locks
- CBRN monitoring devices
- Public address system
- Radio repeater system
- Intercom system
- WiFi system

For further guidance, see:

- SGSecure tip sheet “Protect your customers and IT data”
- SGSecure “Guide for Workplaces,” Chapter 2
- Dutch National Cyber Security Center (NCSC) “IT Security Guidelines for Mobile Apps”

IT_Security_Guidelines_for_Mobile_Apps.pdf.

- ISF Information Risk Assessment Methodology 2

www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

- Global Cyber Alliance (GCA) – February 2019 Cybersecurity Toolkit for Small Businesses
- UK IASME Governance Standard (UK) – for small to medium sized organizations

https://iasme.co.uk/wp-content/uploads/2018/01/IASMEStandardv5.pdf

- CIS Version 7 controls

www.cisecurity.org/controls/

- AON 2019 Cyber Security Risk Report

5 | To help clients maintain cyber security, consider offering only secure access to WiFi at your convention center, rather than (also) free, open-access WiFi.

6 | To manage serious cyber disruptions of core convention center or core client digital services, have the IT Department organize a form of Cyber Emergency Response Team (CERT), either on its own or through a contract / on-call service.

7 | As part of the CERT Business Continuity Management and Crisis Management (BCM/CM) planning effort, consider alternative IT software, hardware and firmware systems to replace capability in case of cyber attack/denial of service.

8 | To help handle serious data breaches, consider having a set, predetermined protocol on how to report a data breach: who will report, how, to whom, in what conditions/ circumstances when an IT data breach is discovered. This so that in the event of a 'hack' or other serious data loss incident, your management has clarity on what needs to happen, by when, in terms of meeting your legal, compliance, duty of care and good stewardship obligations. This is increasingly important as laws and regulations in many countries are expanding of late on this point, including the 2018 introduction of the EU's GDPR legislation, with global implications. This makes informing the right parties appropriately a race against the clock in many situations, making proper preparations that much more important.

9 | To help protect (major) events under special or heightened threat, consider using or hiring social media and or Dark web monitoring tools/services, provided all proper legal and privacy constraints and compliance requirements are observed. An increasingly large number of cyber security, cyber monitoring and cyber security firms as well as more mainstream international security companies run such services.

Tactical Level
Cyber Security Measures

10 | To protect against the unauthorized release of sensitive data, including client event information and data on colleagues that might be used for fraud and other scam purposes, write up and roll out a social media use policy for staff and contractors that outlines rules they should observe on what work-related information they are and are not allowed to post on social media.

11 | To promote a staff and visitor digital hygiene and security awareness culture, use signs, stickers, flyers and posters with simple phrases of the "If you see something, say something" variety, but then geared towards cyber rather than physical threats.

12 | To help protect other convention center stakeholders like suppliers/vendors, hotels and transportation companies whose digital domain may at some point interact with that of your convention center, consider directing them towards Best Practice resources to help themselves secure their IT operations better. For guidance, see:

- Global Cyber Alliance (GCA) (February 2019) – "Cybersecurity Toolkit for Small Businesses"
- Virginia Allen, Partner, Dentons UK & Middle East (March 2018) – "CPNI Employee IT Monitoring Insider Threat."

13 | To ensure that electronic security measures help cover potential cyber security measures, consider having CCTV coverage of all wall and ceiling-mounted WiFi pods (an electronic measure in support of cyber security).

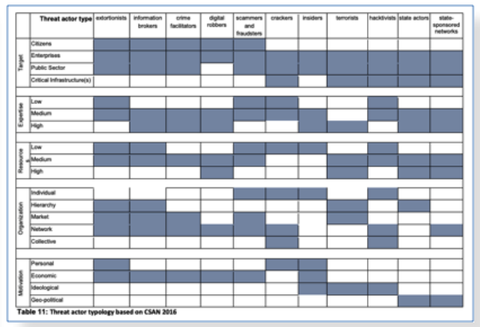
Operational Level
Cyber Security Measures

14 | For information on anti-virus Apps to share with staff for optional use, see 'How to Choose an Anti-Virus App,' www.csa.gov.sg/gosafeonline.

15 | Provide IT staff awareness training on 'crime as a service' concepts, models and means so they have a deeper understanding of how criminal networks worldwide, large and small, misuse software vulnerabilities and apply social engineering to offer services used by a growing number of non-digitally savvy criminals.

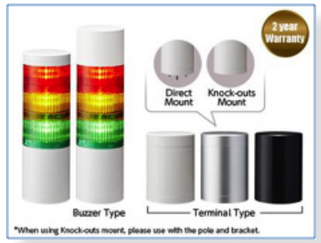
This includes efforts to deny access to information, to corrupt information (impact its integrity) and to steal information. Select in-depth IT staff cyber threat awareness documents:

16 | To help raise awareness about cybercrime actors and their motives, consider having IT staff review the "Towards a New Cyber Threat Actor Typology" (2016). See: www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf



17 | To assist IT and non-IT staff present in the office in being alerted to a significant cyber incident, consider installing a software and 'stacking light' (or 'tower light' or 'stack light') desk lamp designed to go off when a problem is detected by automated software. This to augment other forms of warning, like email, text or WhatsApp message, with a visual form of alert that multiple people can readily spot, and react to.

Examples of the types of available stack light configurations such as the Patlite NHL Network Monitoring LED Signal Tower are shown in the following images:



Additional Resources

Select organizations that AIPC members consult, belong to or that may otherwise serve as a useful resource for security expertise applicable in the convention center and event management sector include (international unless otherwise noted):

- ASIS International
  - Commercial Real Estate Council
  - Fire and Life Safety Council
  - Global Terrorism, Political Instability and International Crime Council
  - Hospitality, Entertainment and Tourism Security Council
  - Law Enforcement Liaison Council
- Association of Event Venues (AEV)
- Australia – New Zealand Counter Terrorism Committee (ANZCTC) (Australia/NZ)
- Business Continuity Institute (BCI)
- Center for Internet Security (CIS)
- Centre for the protection of National Infrastructure (CPNI) (UK)
- Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) (USA)
- Cross-Sector Safety & Security (CSSE) (UK)
- Cybercrime Security Forum (CSF)
- Cybersec European Cybersecurity Forum (CECF)
- European Arena Association (EAA)
- European Cyber Security Organization (ECSO)
- European Major Exhibition Congress Association (EMECA)
- Event Safety Alliance (ESA) (USA – Canada)
- Exhibition and Event Association Australasia (EEAA)
- Exhibitions and Meetings Safety and Security Initiative (EMSSI) (USA)
- Exhibition Services & Contractors Association (ECSA) (USA)
- Global Counter-Terrorism Forum (GCTF)
- Global Cyber Alliance (GCA) (US-UK)
- Information Security forum (ISF)
- Information Systems Security Association (ISSA)
- International Association of Exhibitions and Events (IAEE)
- International Association of Venue Managers (IAVM)
- National Arena Association (NAA) (UK)
- National Center for Spectator Sports Safety and Security (NCS4) (USA)
- National Counter Terrorism Security Agency (NCTV) (Netherlands)
- National Counter Terrorism Security Office (NACTSO) (UK)
- National Cyber security Centre (UK)
- National Institute of Standards and Technology (NIST) (US)
- Overseas Security Advisory Council (OSAC) (US)
- Risk and Insurance Management Society (RIMS)
- SGSecure (Singapore)
- Sports Grounds Safety Authority (UK)
- Venue Management Association (Australia)

Appendices

APPENDIX 1 | Methodology

Over December 2018-April 2019 the AIPC Security Task Force sought draw together a maximum of high value, practicable insights from a diverse, qualified pool of sources in a minimum amount of time. This was done using a process that consisted of the following steps:

1 | Establishment of a data collection research framework defining the scope, types, utility and verify-ability of the information sought;

2 | Collecting data from AIPC Security Task Force members and a range of relevant organizations, institutions, and other depositories of good practice data;

3 | Researching and verifying collected data on quality, validity and overlap for inclusion in the guidance document via comparison and network engagement;

4 | Formatting of data into an initial guidance document;

5 | Cross-vetting of data with feedback loops among Task Force members;

6 |Drawing up final first version of the guidance document.

While the term ‘convention centre’ was at the core of the information gathered, folded into the guidance on security measures are good practices that (also) apply to event and exhibition management, to cyber security generically, to hotel/tourism security, to logistics, to transportation and to VIP or executive protection, all topics that to a greater or lesser degree align with convention centre operations.

The format to present the guidance was drawn from several international standards. The information is divided into five types of measures:

1 | Organizational Security Measures

2 | Physical Security Measures

3 | Electronic Security Measures

4 | Human-based Security Measures

5 | Cyber Security Measures

Within these five sections, where feasible and logical, measures were grouped from the larger strategic to the smaller operational and yet smaller tactical perspective. Where practicable this was done according to the three phases format common to the events sector, namely measures to take before, during and after an incident. This approach deliberately aims to encapsulate the five security functions or phases found in many international security standards and government security strategy documents, namely ‘Deter, Detect, Delay, Respond and Mitigate,’ or ‘Prevention, Preparation, Protection, Response and Recovery.’

OFFICIAL - revised on 19 April 2018

Graduated Security Plan (GraSP)

The primary principle is to maintain business as usual and application of the GraSP should be proportionate, practical and pragmatic

UK TERRORISM THREAT LEVEL	UK ALERT STATUS	THE VULNERABILITIES **People** – Service users, patients, visitors, contractors, customers and staff.	**Physical assets** – buildings, contents, equipment and sensitive materials.	**Information** – IT systems, online transaction systems, electronic and paper data.	**Processes** – Decision making, supply chains, partnership working, critical procedures and production cycle.
LOW Means an attack is unlikely	**NORMAL** Routine Protective Security Measures to appropriate to business concerned	1. References taken pre-employment checks for , agency and volunteer staff 2. Risk assess shared buildings Local authority/Health 3. Fire Risk assessments complete 4. Staff induction for new starts 5. Identity badges issued and worn 6. The primary principle is to Returning of badges and uniforms of retirees or staff leaving organisation 7. Highlight and promote awareness to staff on Fire , Bomb and Suspicious packages procedures, routes and muster points 8. Regular Health and Safety compliance inspections and checks 9. All staff drilled on " Emergency Evacuation" procedures – Fire, Bomb, Chemical 10. All pupils drilled on " Emergency Evacuation" procedures – Fire, Bomb, Chemical 11. All PVG cleared staff given PREVENT training on FLO 12. All supervisors with safeguarding responsibilities to attend the Workshop to Raise Awareness of PREVENT (WRAP).	1. Reception staff ensure secure area Visitor and contractor sign-in/out and ID badges worn. Lost badges de-activated 2. Promote Clear desk policy for office staff and document security protocols 3. Door entry codes changed regularly, secure area keys kept safe and accounted for 4. Organisational assessment of high value assets 5. Develop lockdown protocols and plans 6. Service vehicles parked up in secure areas with keys locked away. 7. Regular walk round security checks in high value asset areas 8. Invite police Security/CT officers to carryout pro-active security assessment 9. Procedures in place to ensure security and integrity of high value assets	1. Perimeter protection is in place and active 2. Lock screen procedures applied by staff when leaving computers unattended 3. Data protection and ICT training for all staff 4. Ensure laptop "Kensington Lock" process is followed where appropriate 5. Apply document classification scheme where applicable 6. IT and data protection requirements re-enforced to all staff annually 7. Regular password changes required. 8. Secure email system in place for key staff 9. Staff are made aware of responsibilities relating to information handling and cyber security threats 10. Staff sign acceptable use policy 11. Technical staff maintain an appropriate patching & update regime for all council ICT hardware	1. Identified Lead Officer in place with responsibility and accountability for Security policies and protocols 2. All existing security guidance considered and applied appropriately Procurement background checks 3. Directors to ensure Business Continuity plans are in place, approved and tested 4. Risk assessment and safe working procedures for staff and processes inc buildings, receptions, mail rooms, vehicles, fuel storage, vulnerable equipment and materials 5. Telephonist and reception staff trained in actions to be taken on receipt of a bomb warning 6. Check posters and advice is in place and displayed in appropriate areas for dealing with bombs and suspicious packages and tailgating through secure doors 7. Procurement background serious organised crime checks to providers Call centre staff, school office staff, trained in actions to be taken on receipt of a bomb warning 8. Check posters displayed for bomb and suspect mail identification and action 9. Check correct blank forms readily accessible to record details of bomb threat
MODERATE Means an attack is possible, but not likely					
SUBSTANTIAL Means an attack is a strong possibility	**HEIGHTENED** Additional and Substantial protective security measures, reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.	As above plus 13. Invoke strict compliance with badge wearing and identification policies, promote tailgating awareness 14. Highlight risk assessment and reporting processes to encourage staff awareness and responsibilities 15. Strict control and approval for issue of temporary passes 16. Promote **"run-hide-tell"** video to all staff 17. Regular building security housekeeping checks 18. Re-inforce awareness and understanding of Fire and suspicious Package procedures 19. All staff briefed on Anti-terrorist hotline 20. Review staff higher level security access as "essential only" 21. All staff drilled on "lockdown" procedures 22. All pupils drilled on "lockdown" procedures 23. Promote CITIZEN Aid App to all staff	As above plus 10. Ensure building/office search and clearance processes in place Procedures in place to ensure security and integrity of risk assets with building search and clearance processes in place 11. Deliver and promote **Project Griffin** to key staff (Initiative for organisations to protect staff and communities from terrorism) 12. Promote **Anti-terrorist hotline (0800 789 321)** to staff 13. Regular leadership security housekeeping checks inc. testing of security equipment 14. All HGV drivers to read and comply with NaCTSO Education leaflet/poster – "**keep your heavy goods vehicle secure to help reduce criminal activity**"	As above plus 12. Invite accredited security partners to test our perimeter protection including web filter, web presence and network perimeter 13. Technical staff reminded of cyber security requirements 14. Implement CISP (cyber security information sharing protocol 15. CERT standby	As above plus 10. SLT to participate in LRP "Move to Critical" planning workshop 11. Evaluate and develop move to Critical Planning 12. Police briefing to SLT on 'Emerging and Local Threat Profile' 13. Business Continuity Plans tested every 12 months and approved by HoS
SEVERE Means an attack is highly likely					
CRITICAL Means an attack is expected imminently	**EXCEPTIONAL** Maximum protective security measures to meet specific threats to minimise vulnerability and risk	As above plus consider these Tactical Options depending on any identified specific regional or sectoral threat assessment: ✓ Comms. Unit/Duty Resilience officer to Circulate and re-inforce HM Govt. S Govt and Police Scotland public safety messages to Managers and Supervisors ✓ SLT to implement strict adherence by all stakeholders to all security measures, including that visitors and contractors to be escorted at all times ☐ On notification of any move to critical during office hours, the Comms Unit and O of Hrs, the Duty Resilience Officer, will circulate two pre-scripted Leadership messages 1. to all staff (be alert but not alarmed - do 3 things now) 2. to all lead tenants and Managers (your leadership is required - do 5 things now) ☐ Director CYPLL to consider implementing a communications strategy to provide advice pupils and parents ☐ SLT to consider implementing firm application of lone working arrangements ☐ SLT to consider cancelling non-essential travel and out of region school and business trips ☐ SLT to consider ceasing all non-essential services for a period of time ☐ SLT to consider insisting that all meeting start with security briefing Inc. actions to be taken in the event of alarm sounding and route to assembly point ☐ SLT to consider restricting deliveries to essential and expected items only	As above plus consider these Tactical Options depending on any identified specific regional or sectoral threat assessment: ✓ Implement Daily leadership security briefings, reviews and housekeeping checks ✓ To engage quickly with key stakeholders ✓ Ensure that any changes, including return to SEVERE, are communicated to staff ☐ SLT to consider minimising access points to all building ☐ SLT to consider "shrinkage" of building occupancy – non essential staff ☐ SLT to consider cancelling non-essential public meetings ☐ SLT, with LRP partners to consider advising the cancellation of public events ☐ SLT to consider increased monitoring of CCTV and additional car park checks ☐ SLT to consideration of lockdown of sites and maximising security on site ☐ CE or Senior Management Cover ☐ to consider Major Incident Declaration ☐ SLT to consider additional security including parking on site, staff vigilance	As above plus consider these Tactical Options depending on any identified cyber-attack ☐ Implement CERT (cyber security emergency response team)	As above plus consider these Tactical Options depending on any identified specific regional or sectoral threat assessment: ✓ Out of Hrs the Duty Resilience Officer to agree GraSP Strategy with Chief Executive or Senior Management Cover ✓ Resilience Staff to liaison with SLT as appropriate and Head of OD, HR and Assets ✓ Liaison with Scottish Government and Police Scotland ✓ CE or Senior Management Cover to consider immediate and special daily/regular updates to Senior Members / all Elected Members ☐ CE or Senior Management Cover to consider immediate and special daily/regular meetings of Senior Leadership Team ☐ SLT to consider pro-active liaison and communication with partners to highlight potential impacts ☐ SLT to assess risk to service users and stakeholders against threat detail ☐ SLT in consultation with LRP partners to consider immediate threat briefing to Community Planning Partners ☐ CE or Senior Management Cover to consider Communications and Co-ordination with and to Local, Regional and Scottish Resilience Partnership

The three levels of response broadly equate to threat levels. A move to CRITICAL does not infer a move to response level EXCEPTIONAL

The ✓ signifies a pre-determined action, regardless of any specific threat

The ☐ signifies a consideration which can vary depending on the threat assessment

National Stakeholder Menu of Tactical Options

Attack Methodology

Under the Protective Security Improvement Activity (PSIA) introduced by NaCTSO in 2014, six methods of attack have been identified:

- Non penetrative vehicle attack
- Penetrative vehicle attack
- PBIED - Person borne Improvised Explosive device (suicide) attack
- Firearms/Weapons attack – (Marauding Terrorist Attack)
- Postal device attack including courier and hand deliveries
- Placed IED.

The tactics outlined in this document reflect the options for response to these types of threat.

Overall Strategy

The overall business strategy in dealing with an increase in threat level to 'Critical' or in response to an attack is:

To understand the type of threat posed (why did the threat level increase? What was the attack methodology?) and to consider the appropriate level of response and range of tactical options that are best suited to (insert name of contract here) to allow them to continue 'business as usual', within the parameters of this heightened state of alert.

Operational Requirement

The operational requirement to consider when planning for an increase in threat level to 'Critical' is:

- To agree a menu of site specific tactical options that are suitable for your organisation that can be considered if the threat level increases to 'Critical',
- Regularly exercise the plan for 'Critical' to ensure that key stakeholders and staff are aware of the impact on their area of work should a change be necessary,
- Ensure that staff have been consulted and agreements in place if options impact on staff working practices (terms and conditions).

The Operational Requirement to consider when reacting to an increase in threat level to 'Critical' is:

- To escalate and engage quickly with key stakeholders to react when the threat level increases to 'critical',
- To consider the range of options relevant to mitigate the threat posed,
- To continually review the tactical options to ensure they remain 'fit for purpose",
- Ensure that any change to tactical options serve to provide reassurance to staff rather than cause for alarm,
- Implement communication strategy to provide advice to staff around changes to planned events/deliveries/changes to access points etc.
- Only react to information from official sources such as the Government, Security Services and Police as there is a lot of misinformation available through unsubstantiated sources,
- To have an immediate holding plan available to allow a more permanent solution to be found,

- Consider implementing a command and control strategy using the Strategic, Tactical and Operational (formerly Gold/Silver/Bronze system),
- **STRATEGIC** is in overall control of the organization's resources at the incident and will formulate the strategy for dealing with the incident,
- **TACTICAL** manages tactical implementation following the strategic direction given by Gold and makes it into sets of actions that are completed by Bronze,
- **OPERATIONAL** directly controls an organization's resources at the incident and will be found with their staff working at the scene,
- Minimise disruption to business.

Menu of Tactical Options

The following list of tactical options should be considered now to support an increase in threat level to 'Critical' or following an incident or attack.

This is not an exhaustive list and there may be other site specific options which are relevant to your site. The key to any change is that security patrols should remain unpredictable. Feedback from security services has proved that this is a real deterrent when planning an attack.

A	Agree strategy and document all decisions (to include rationale regarding for change or preserving status quo).
B	Ensure lock down procedures are tried and tested.
C	Implement emergency change to shift patterns (extended shift patterns, change to rotation etc. – Agree plan with staff in advance).
D	Review patrol strategy (be unpredictable). Adopt high visibility clothing. (Deployment in Hi-vis will be dependent on the intelligence available and the perceived risk to the site).
E	Brigade resources with neighbouring contracts (rotate and share external patrols with other security companies and widen patrol area).
F	Report any suspicious activity in a timely manner.
G	Implement communication links with surrounding premises to pass on information about suspicious activity/behaviour.
H	Consider closing non-essential access and egress points.
I	Focus CCTV on all communal areas and vulnerable points.
J	Ensure CCTV is fit for purpose.
K	Review immediate parking areas and access to them.
L	All visitors must give 24 hours' notice.
M	Implement search regimes (people, vehicles, baggage, etc.)
N	100% staff ID checks (challenge ALL staff).
O	All staff and visitors to wear ID (if this is not usual practice).
P	Visitors to be accompanied at all times.

Q	Security officers must check all personnel and vehicles including emergency services – do not assume they are who they say they are!).
S	Consider cancelling or postponing events.
T	Cancellation of all non-essential training ensuring staffing levels are maintained.
U	Staff are briefed on response and threat levels.
V	Restrict deliveries to essential deliveries only (out of hours only).
W	Couriers – Essential deliveries only.
X	Post: ✓Where possible 100% scan ✓Ensure postal procedures are robust

Remember, there is evidence to support that strong, robust and vigilant 'communities' provide a hostile environment for terrorists/criminals to operate in.

Useful Links

The following links provide additional useful information that may assist when deploying the tactical options;

http://www.cpni.gov.uk

https://www.gov.uk/government/publications/stay-safe-film

http://www.nactso.gov.uk

http://www.mi5.gov.uk

https://www.gov.uk/government/publications/crowded-places-guidance

MCCA Cyber Security Presentation

MASSACHUSETTS CONVENTION CENTER AUTHORITY

Signature BOSTON

Threat Vectors

Malware
- Ransomware
- Spyware
- Trojans
- Viruses
- Worms

Hacking
- Cross-Site Scripting
- DDoS
- SQL Injection
- Session Hijacking / Man in the Middle

Social Engineering
- Phishing
- Spear phishing
- Watering Hole

MASSACHUSETTS CONVENTION CENTER AUTHORITY | Information Technology | 2 April 2019 | 3

Top 10 Data Breaches 2018

	How Many People Affected	Disclosed
1 Aadhaar Breach	1,000,000,000	January 2018
2 Starwood-Marriot Breach	500,000,000	September 2018
3 Exactis Breach	340,000,000	June 2018
4 Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5 Quora Breach	100,000,000	December 2018
6 MyHeritage Breach	92,000,000	June 2018
7 Facebook Breach	87,000,000	September 2018
8 Elasticsearch Breach	82,000,000	November 2018
9 Newegg Breach	50,000,000	September 2018
10 Panera Breach	37,000,000	April 2018

- Average total cost of a data breach: $3.86 million
- Average cost per lost or stolen record: $148
- Likelihood of a recurring material breach over the next two years: 27.9%
- Average total one-year cost increase: 6.4%
- One-year increase in per capita cost: 4.8%
- Average cost savings with an Incident Response team: $14 per record

MASSACHUSETTS CONVENTION CENTER AUTHORITY | Information Technology | 2 April 2019 | 5

Cyber Security Framework

NIST 800-53
- 18 Control Families
- 115 Security Controls

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS – Personal Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

MASSACHUSETTS CONVENTION CENTER AUTHORITY | Information Technology | 2 April 2019 | 7

Future Initiatives

- DDoS Protection
- Show Firewall
- Mobile Threat Management
- Multi-Factor Authentication O365
- Mandatory Cyber Security Awareness Training
- Network Access Control (NAC)
- Change Management (ServiceNow)
- Windows 10 upgrade
- Windows Server 2016 upgrade
- Polaris (Rubrik)

MASSACHUSETTS CONVENTION CENTER AUTHORITY | Department Name | 2 April 2019 | 10

Signature BOSTON
Remarkable experiences. Imagination realized.

Massachusetts Convention Center Authority

MCCA Vendor Security Guidelines

11.26.2018

I. General

The Massachusetts Convention Center Authority, ("MCCA"), is a National Institute of Standards & Technology, ("NIST"), cyber security compliant organization. Specifically, the MCCA aligns its IT security posture with the NIST 800-53 framework. As such, the MCCA requires that all MCCA contract partners, hereinafter "Vendors", must adhere to the following cyber security guidelines in this document.

II. Security

A. Application Security

If Vendor manages or has access to any application specific to the MCCA, Vendor must implement the following controls:

1. *Authentication*

a) All access is authenticated and communication secured using industry best practices.
b) Systems identity is tied to an individual user by the use of credentials. Second factor authentication will also be used when applicable.
c) Reasonable authentication controls that conform to industry recognized standards are provided.

2. *Authorization*

Vendor agrees to:

a) Ensure that authorized users are only allowed to perform actions within their privilege level.
b) Control access to protected resources based upon role or privilege level.
c) Prevent privilege escalation attacks.

3. *Password and Account Management*

a) Passwords should follow best practices, including:

I. Encrypting passwords using "hashing" and "salting" techniques.
II. Enforcing password complexity.
III. Limiting failed attempts before account lockout.
IV. Not allowing clear passwords.
V. Password reset does not send credentials.

b) Where appropriate, Vendor shall securely log (with time and date) commands requiring additional privileges to enable a complete audit trail of activities.

B. Data Security

Vendor shall implement the following best practices:

1. *Password and Account Management*

a) MCCA Data is encrypted using industry best practices.
b) Backups of MCCA Data have the same controls as production data.

2. *Data in Motion*

a) MCCA Data in transit to or from MCCA will be encrypted (e.g., SFTP, certificate-based authentication).
b) MCCA Data sent over browser should use SSLv3 or better.

3. *Multi-Tenancy*

a) In a multi-tenant environment, Vendor shall provide appropriate security controls and robust cryptographic methods to protect and isolate MCCA Data from other tenants.

4. *Administrative Access and Environmental Segregation*

a) Applying Principle of Least Privilege: Proper controls should be in place to ensure that access is limited to administrators who must see MCCA Data in order to fulfill their job functions.
b) Where possible, confidential data should be masked with one-way hashing algorithms.
c) MCCA Data should not be replicated to non-production environments.

C. Threat Management

Vendor shall implement the following best practices:

1. *Intrusion Detection*

Vendor shall implement measures to ensure that the MCCA is alerted when the system or service detects unusual or malicious activity. Vendor shall notify MCCA immediately regarding any significant intrusion.

D. Infrastructure Security

Vendor shall configure the infrastructure (e.g., servers and network devices) and platforms (e.g., OS and web servers) to be secure following these best practices where applicable:

1. *Audit Logging*

a) Vendor shall log all system access to the MCCA's Service to produce an audit trail that includes, but is not limited to, web server logs, application logs, system logs and network event logs.

2. *Vulnerability Management*

Vendor shall implement commercially reasonable processes designed to protect MCCA Data from system vulnerabilities, including:

a) Application Vulnerability Scanning: Vendor shall perform application vulnerability scanning on the Vendor's Service before code is released into production. Vendor shall produce reports reasonably promptly thereafter and make them available to MCCA on request.

b) Malware Scanning: Vendor shall perform anti-malware scanning on all servers utilized in performing the Vendor's Service.

E. Security Procedures

Vendor shall implement the following best practices:

1. *Incident Response*

Vendor shall maintain security incident management policies and procedures, including detailed security incident escalation procedures. In the event of a breach of any of Vendor's security or confidentiality obligations, Vendor agrees to notify MCCA by telephone and email of such an event within twenty-four (24) hours of discovery. Vendor will also promptly perform an investigation into the breach, take appropriate remedial measures and provide MCCA with the name of a single Vendor security representative who can be reached with security questions or security during the scope of Vendor's investigation.

2. *Patch Management*

Vendor shall use a patch management process and tool set to keep all servers up to date with appropriate security and feature patches.

3. *Documented Remediation Process*

Vendor shall use a documented remediation process designed to timely address all identified threats and vulnerabilities with respect to the Vendor's Service. High severity findings should be reported to MCCA and remediated within thirty (30) days.

4. *Employee Termination Procedures*

Vendor shall promptly terminate all credentials and access to privileged password facilities of a Vendor employee in the event of termination of his or her employment.

F. Governance

Vendor shall implement the following best practices:

1. *Security Training*

Vendor shall ensure that all Vendor employees and managers complete relevant training required to operationalize the procedures and practices outlined herein, including security awareness training, on at least an annual basis.

3. *Security Reviews*

Senior-level managers of MCCA and Vendor shall meet at least once annually to discuss: (1) the effectiveness of the Vendor's security platform; and (2) any updates, patches, fixes, innovations or other improvements made to electronic data security by other commercial providers or for other customers of Vendor that Vendor or MCCA believe will improve the effectiveness of the Vendor's security platform for the MCCA.

4. *Third-Party Audits and Compliance Standards*

a) Vendor shall provide MCCA with a copy of any security audit (including SSAE 16, AICPA Service Organization Control Reports or independent audits) that is performed no more than thirty (30) days after Vendor receives the results or reports.
b) [PCI-DSS COMPLIANCE IF APPLICABLE]

Vendor shall maintain policies, practices and procedures sufficient to comply with the Payment Card Industry Data Security Standard, as the same may be amended from time to time, with respect to the Vendor's Service and subject to request by the MCCA.

G. Physical Security

Vendor shall implement the following best practices:

Vendor shall limit access to its facilities utilized in performing the Vendor's Service to employees and employee-accompanied visitors using commercially reasonable Internet industry standard physical security methods. At a minimum, such methods shall include visitor sign-ins, restricted access key cards and locks for employees.

_____

Vendor Signature

_____

Date

EXCELLENCE IN
CONVENTION CENTRE
MANAGEMENT

aipc.org