Exercise CyberSmart 2017

Exercise Summary Report

Sponsors:

USA:
Crawford
Hope Foundation
Miller Ingenuity
UPS
WELLSTAR
WSB-TV2 Atlanta

Regional Sponsors, Australia:
Audeamusrisk
Tank Stream Labs
Avalias

Regional Partners, Australia:
Australian Women in Security Network (AWSN)

Report prepared by:

Foreword from Len Pagano, President of SafeAmerica/WorldSafe

The subject of Cyber Security is an important one in the minds of leaders in every organization today. The rapid rise in cyber-attacks - with high-profile companies and government agencies having been affected in the USA and abroad - makes this subject a focal point that formed one of the key areas of attention at our Training for Safety Conference in Atlanta in October this year.

This is the first exercise of its kind that SafeAmerica/WorldSafe has delivered to the business and government communities in conjunction with this high-profile conference and extended exercise event.

On behalf of the SafeAmerica / WorldSafe Board and the team I extend my thanks to all those that attended the conference and those that participated in the exercise in each of the five cities. Also, a big thank you to the Exercise Team for their great support and dedication in delivering an excellent exercise. We were also fortunate to have Harold Wolpert and Avalias donate their services and exercise delivery software to help make this event a success. The success of the exercise was itself an illustration of teamwork and technology working together.

We hope that you find this report an interesting compilation of the outputs of the discussions that took place, and we look forward to you supporting and participating in future SafeAmerica and WorldSafe events.

A Message from the Exercise Director, Harold Wolpert

Exercise CyberSmart reflects a necessary global shift, whereby organizations are focusing on effective preparedness as a means of reducing risk. With this exercise, we set out to provide a forum for organizations across industries and disciplines to share best practice and take away ideas to improve their organizational readiness for cyber security incidents.

To acknowledge the global nature of cyber risk, we brought together multiple cities across the world, selecting New York, Washington DC, London UK and Sydney Australia to join Atlanta, as major cities that could potentially be affected, as was experienced in the WannaCry ransomware attack earlier this year.

The importance of communication was a recurring theme in the discussions, and the exercise reminded us that there are others to turn to for help, guidance and support; both in preparation for, and during such an incident.

It was inspiring to see such active involvement from so many people during the exercise. This unfaltering commitment to preparedness will help to ensure that our societies are as resilient as possible in the face of global threats. On behalf of the Exercise Team, I'd like to thank our valued participants, along with the hardworking team and sponsors who helped make Exercise CyberSmart a success.

WorldSafe Cybersecurity Exercise – "Exercise CyberSmart"

Exercise Name:	**Exercise CyberSmart 2017**
Exercise Date:	**October 25/26, 2017** (3 time-zones across UK, USA, Australia)
Exercise Type:	**Tabletop Discussion Exercise**
Facilitated by:	**Harold Wolpert** (CEO, Avalias & Exercise Director)
Project Team:	**Doug Himberger, Harold Wolpert, Jessica Robinson, Kathleen Lucey, Nelson (Skip) Riddle, Ted Waldbart**
Delivery Team:	**Doug Himberger** (SafeAmerica Board Member / Project Member / Atlanta Facilitator) **Harold Wolpert** (Avalias CEO / Exercise Project Leader / Global & Sydney Facilitator) **Jessica Robinson** (Purepoint / Project Member / Cycurity Lead) **Ted Waldbart** (EVP Operation SafeAmerica / Logistics and Administration) **Nelson (Skip) Riddle** (Riddle International / London facilitator) **Joe Hernandez / Carol Gabel** (New York Facilitation Team) **Jena Roscoe** (Hope Foundation / Jessica Hoffman PWC / Washington DC Facilitation Team) **Dave Wolpert** (Avalias CTO / Avalanche TTX Scenario Delivery / Global Exercise Controller) **Len Pagano** (President SafeAmerica Foundation / Project Owner)

Introduction

Exercise CyberSmart was a discussion-based tabletop exercise, focussing on the strategic issues that need to be addressed by organizations during a cyber-attack. It was conducted concurrently across five cities and three timezones, involving participants in Atlanta, New York, Washington DC, London UK and Sydney Australia.

The exercise simulated a large-scale coordinated cyber-attack on critical infrastructure sectors, including the banking system, information technology (IT) and communications. At first, the attack appeared to be contained to organizations' local regions, with it later becoming clear that the attack was affecting organizations worldwide. The scenario's premise unfolded towards the end of a day, at a time when various customers' important quarterly processing was supposed to be taking place.

Participants represented a broad cross-section of roles, responsibilities and organizations. These included leadership from large and small business; federal, state and local government; educational institutions; public safety; and not-for-profit organizations. Subject-matter experts spanned the fields of disaster management, banking, cyber-security and business continuity; offering a wide breadth of knowledge and experience that provided valuable shared learnings.

Exercise Aim

The exercise aimed to increase the awareness of the strategic issues faced by both the public and private sectors during a major cybersecurity incident. Through discussion of a simulated large-scale coordinated global cyber-attack on critical infrastructure organizations, the exercise aimed to examine and share understanding of the strategic level processes, procedures, tools, and response options available to organizations of various types.

Exercise Objectives

Objective 1 – For each organization to consider their capabilities to prepare for, protect from, and respond to the potential impacts of cyber-related attacks.

Objective 2 – For each organization to consider processes and procedures relevant to their specific industry – in relation to controlling the situation, informing authorities and sharing sensitive information across state, local, national and international boundaries, sectors and partners without compromising proprietary or national security interests.

Objective 3 – To validate information sharing relationships and communications paths for the collection, reporting, retention and dissemination of situational awareness during a cyber incident, including response and recovery information.

Objective 4 – To exercise strategic decision making and encourage working together with other agencies and organizations to support the coordination of incident response(s) in accordance with your organizational or government policies and procedures.

Exercise Scope

The exercise focused on the strategic issues that need to be addressed, and not the details of the technical response. Due to time constraints, this scenario did not address the specific considerations of each individual organization. As a discussion-based exercise, functional response activities were not exercised.

Discussion Outcomes – Response to a Cyber-Attack

The outcome of the discussions by participants during this exercise are outlined below.

Importantly, these outcomes represent an amalgamation of multiple organizations' opinions and approaches to a cyber incident, which means they may contain points that are not applicable or suitable for your organization.

As such, the findings should be used as a source of ideas, rather than as a single source of best practice, when reviewing your organization's plans and procedures.

Initial Actions

The following suggestions were given as initial actions that would be taken by various organizations upon receiving notification that a cyber-attack was underway. The points raised may not apply to organizations of all sizes:

- Activate your Cyber Response Plan.
- Assemble your Cyber Response Team, which should include representation from all areas of your organization. Some members may be in other parts of the region.
- Identify the scope and scale of the attack – is it local or regional?
- Involve Public Relations early to manage your key messages to all stakeholders, including employees.
- Lay out the facts – what you know and what you don't know. You should expect the team to do this.
- Avoid relying on email or other Internet-based communications methods to share information.
- Keep the relevant executives notified when response actions have been implemented.

In addition, the following suggestions were made regarding preparations that should occur prior to an event of this sort occurring:

- Identify in advance which of your stakeholder teams should be alerted in the event of this type of major incident.
- Have a Cyber Response Plan in place.
- Engage in advance with external service providers you may need during an incident such as cyber security technical specialists and disaster recovery experts.
- Include in your plan a list of external service providers that you would call for assistance during an incident.
- Prepare notification lists in advance, to accelerate communications in the early stages of an incident.

Notification Processes

The discussions identified the following suggestions and issues regarding internal and external notifications upon finding out about the cyber-attack:

- An initial message could be sent out to internal teams with the following key information: *"Please advise your stakeholders that we are identifying the problem and seeking to isolate it. We are also in contact with our customers and suppliers asking them to be patient and weather this storm with us. Our employees are aware of the issue and will support them through the incident."*
- Organize response team with different disciplines, and ensure that a leader has been appointed.
- Quickly prepare messaging once attack has happened, and as an understanding of the situation evolves.
- Engage employees, customers and suppliers early on, also engaging other stakeholders as needed.
- For some organizations, the CEO decides on all out-bound communications at speed. Identify who would be responsible for this in your organization.
- For organizations in the European Union (EU), it is important that all members are trained and knowledge of in-situ principles and behavior assessed, particularly given new General Data Protection Regulation (GDPR) legislation.

Inbound and outbound notifications

The following key internal stakeholders were identified as requiring regular communications, both as sources of information and as recipients of updates:

- IT Department
- Customer Service Teams
- Major Account Reps
- Communications Team
- Legal and Financial
- All clients - VIPs and others
- The board will be alerted if the situation escalates.
- Your insurance company - when you contact them, tell them what coverage you have, and mention that there is no physical damage – note, some organizations may have specific Cyber insurance
- *Note: this is not an exhaustive list*

Significant recurring themes

Multiple sources emphasized the importance of **having a unified voice that must be echoed throughout all communications**.

Issues facing the organization

Exercise participants in each city were divided into groups representing four different functional areas, and asked to identify the key issues facing their areas of focus.

Based on a consolidation of these discussions, the following lists of strategic issues were identified, noting that some issues may have been overlooked due to time constraints:

Finance / Legal / Insurance / Investor Relations

The following issues were identified relating to these functional areas:

- Which systems are working? Do they require additional protection?
- Which systems are down? Do we know why?
- Who needs to know? (e.g. Management, Insurance Brokers, Regulators)
- What external / government help is available?
- Handling the lapse in operations with customers and suppliers.
- Liability.
- Coordination between departments.
- How to demonstrate to customers that leakage of their data can be controlled?

Information Technology / Network Management / Telecommunications / Cyber-Technical Specialists

The following issues were identified relating to these functional areas:

- Early detection and rapid response
- How to ensure that affected systems and servers are isolated and secured before viruses are spread
- Communications: Internal; Management; IR Coordination; IT Staff
- Continuity of Business (COB) for each Line of Business (LOB)
- Monitoring: US Cert / Systems Monitoring
- Transaction Monitoring / Batch Pausing

Other interesting comments regarding priorities and important areas of focus:

- The top priority is engagement. Helping to scope the issue, such as who has access and who doesn't have access could provide intelligence about the nature of the attack.
- The Incident Response Plan is very important in this type of situation.
- Preparedness is important, including organization, training and investment, auditing, ISO certification, and other areas.
- With preparedness activities, there should be a focus on coordination with other departments and training frequently, as new malware arises.
- The question needs to be asked: does the cloud help mitigate risks?

Sales / Marketing / Customer Services / Customer-Facing Roles

The following issues were identified relating to these functional areas:

- Establishing a communications protocol with the Executive team, related to the Sales Teams that are client-facing.
- Getting access to a company-approved response to the security breach.
- Establishing a FAQ for internal and external use.
- Data gathering to determine potential liabilities to the customer and any legal implications.
- Establishing a proactive approach for protecting the reputation of the company.
- Coordination across departments.
- Rapid response ability; authority from CEO and when it must escalate to CEO directly.
- Being open and honest about what we can control and what we cannot control.

Some additional points were raised regarding the importance of preparedness, in advance of such an incident occurring:

- Have a communication plan ready for customers / suppliers / stakeholders.
- Consider also preparing with your customers and suppliers... are they ready?

Other interesting comments regarding priorities and important areas of focus:

- Supply chain management will also immediately be impacted, but later resolved.
- This won't only affect banking – it will trickle into other parts of the supply chain.

Operations / Security / HR / Communications / Public Relations / Media (Internal & External) / Law Enforcement

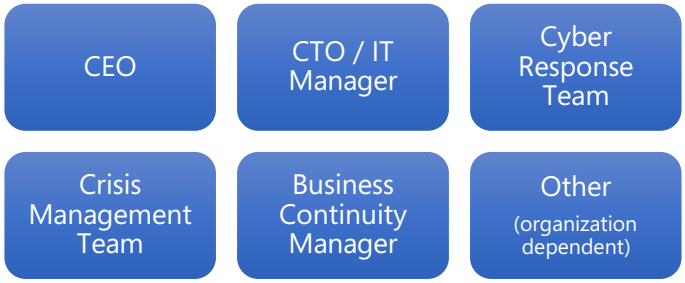
The issues identified as facing these functional areas were provided as a top priority for each relevant group, as follows:

- **Operations:** Not knowing whether any transactions can be carried out at this stage.
- **Security:** Closings of banks; safety of employees and data; securing info and data.
- **Human Resources:** Payroll, and communication to employees and vendors.
- **Public Relations:** How to communicate to media, and what is the message.
- **Law Enforcement:** How to secure banks / protect what is in them / close the vaults.

Who is in control?

Depending on the size and nature of the organization and industry, different roles and/or groups may take the lead in managing the crisis.

In the context of the scenario presented to participants during this exercise, the discussions identified the following roles or groups that may take control during such an incident:



Some noteworthy comments that came out of the discussions of who is in control:

- In cases where the CEO is not in control, for example when the Crisis Management Team has command and control, the CEO may want to have Counsel and their PR team present for the Crisis Management Team briefings.
- The CEO cannot play a passive role, even if they're not in control of the incident.
- It can be advisable to seek Outside Expert General Counsel.
- The CEO would coordinate, and this is an "all-hands-on-deck" situation.
- If there is no longer a cyber risk, the COO may take control. This also depends on whether the issue is local/regional.
- In this scenario, the U.S. Department of Homeland Security (DHS) would be active. In other jurisdictions, local government agencies and/or law enforcement agencies would be active.
- Trade groups may also come into play.

Executive-Level Issues

The following were identified by participants as important factors that should be considered by the Executive when dealing with such an incident:

- **Response factors:**
  - Ensuring that employees are notified and know their roles.
  - Ensuring clients are handled if service is necessary.
  - Ensuring prompt communication with frequent updates.
  - Regular assessment of impacts
- **Impact factors:**
  - Personally identifiable information leaks
  - Protected health information leaks
  - Identity theft and fraud
  - Export/import trade issues
  - Cascading impacts to unaffected businesses
  - Potential delays with payroll
  - Continuity with mission critical vendors
- **Other factors:**
  - Complicated/varied global regulations
  - Reputation

Activating your Business Continuity and/or Cyber Response Teams

Depending on the type of organization, the process for activating Business Continuity and/or Cyber Response teams may vary. From discussions during the exercise, the following common steps and considerations were identified (in no particular order):

- **Set up incident command.**
  - This may be specialized for cyber response, based on an already established protocol. Often this is connected to the Business Continuity Team.
  - For some organizations, when there is an incident, they automatically assemble a team in their building or a nearby hotel.
- **Set up primary and alternative communication methods.**
  - Set up a call station, and call in with a contingency plan.
  - When choosing alternative communication methods, remember that Internet-based systems may not be functioning normally during a cyber-attack.
- **Assess the extent of the problem, and contain it.**
  - Identify what is broken.
  - Identify what you know and what you don't know.
  - Take steps to contain the problem on those servers affected and isolate them.
- **Notify customers and suppliers.**
  - First find and consult with a general counsel.
  - Then craft the message that will go out in communications to customers.
  - It is essential to have a 'unified voice' that must be echoed throughout all communications.
  - Key account managers should phone customers and VIPs to alert them.
  - Operations should phone key suppliers regarding settlement delays.
- **Advise the board, and employees, of problem and actions.**
  - Provide the board with information regarding the problem and what is being done.
  - Human Resources should advise employees.
  - The board and employees should be asked to answer external questions with "we are aware of the problem and are handling it".
- **Legal/Financial should advise your insurance company.**
  - When you notify them, tell them what coverage you have, that the incident does not affect anything physical.
  - Some organizations have specific cyber insurance for these types of incidents.
- **Legal/Financial should advise financial authorities.**
  - As an example, in the UK this is Financial Services Authority (FSA).
- Third-parties should be directed to a Public Relations member of the Cyber Response team as a liaison point.

Role of the Board, Executive Team and the Cyber Response Team

Based on discussions, the following points were raised regarding the role of the Board, Executive Team and the Cyber Response Team:

- Maintaining trust among customers.
- Mitigating the risk of customer data leakage and regulatory consequences
    - In the EU, regulatory consequences can mean as much as 5% of annual revenues.
    - In the US, such leakage has already cost one of the organizations present $595,000 in penalties.
- Preparation is key. While we can minimize risks, we cannot prevent an incident of this type, so we need to be prepared and able to respond quickly and effectively:
    - Do we have the right people in place?
    - Have they been trained?
    - Systems and processes?
    - Business Continuity templates/procedures?
- The Board needs to be informed, and have accountability. Procedures should be in place and the Board should assess these.
- Balancing the need to innovate "smarter" products, given that this generally means they are connected, and this creates more risk.
- Some see the cyber-security arena as an "Arms Race".

  (Due to time constraints, this discussion was cut short, however these roles are discussed in more detail through other sections of the report.)

Changes to strategic communications priorities

Participants discussed different ways of thinking about strategic communications priorities, resulting in the following comments:

- It is important to address internal-facing communications, not just external. Rumor control can make a big difference to the impacts on the organization.
- Planning for communications is important, because when a real incident occurs, getting the right messages out quickly to the right people will be important.
- One idea is to make videos to reassure customers, and to provide a clear message of stability for both employees and customers to alleviate their concerns.
- The more robustly prepared your social media team is prior to an incident, the better off you'll be.
- For communications, as with other response factors, the best way to prepare is to practice, practice, practice.

Pre-arranged experts

The participants raised that subject-matter experts are often pre-arranged to assist the organization with the response to a cyber-attack. These include:

- Expert outside counsel
- Outside incident response teams
- Companies that can help you patch security flaws
- Cyber breach coach

Effective media management

The following key themes were raised in relation to effective media management:

- The media can amplify realities and cause people to panic and disrupt other systems.
- It is important to keep in mind that an incident of this nature isn't just about us but all our stakeholders and, probably, a wider community that have been affected.
- Keep feeding the media with updates and developments, otherwise they will use alternative sources that may cause unnecessary damage your organization.
- Remember, the incident affecting your organization may not be the entire incident – keep monitoring media throughout the incident, and follow your industry guidelines.
- Remember the people responsible for the attack may be watching the response and using the information to their advantage.
- Cyber-attack is a crime, and Police need to be notified immediately.
- A phone call to Police can put you in touch with relevant parties in other jurisdictions.

General

The following other general themes were raised in relation to media management:

- Have a believable media spokesperson (CEO or recognized leader).
- Brief staff well and frequently.
- Create a single source of truth - avoid different communications from different sources (needs to be defined as a key part of the Cyber Response Team)
- Engage as soon as possible with Government – depending on your industry, they may be the best channel to communicate with the media.
- Use communication to instill confidence - "no message is a message".
- Remember to communicate with employees to reassure them as well.
- You may need to adjust your planned approach based on the situation.
- Be honest – don't distort the facts, they will come out eventually.
- Answer the questions you can, and ask for patience for those you cannot.
- You might have to dispatch media personnel to different locations.
- Monitor regulator messaging.

Social media

The following suggestions and considerations were raised regarding social media during an incident of this type:

- Social media is faster than traditional media.
- Social media is often the first place your customers go for information.
- Make sure your Cyber Response Plan has a section on Social Media management.
- Have policies for in-house use of personal social media during any incident.
- Make sure that your social media accounts are secure.
- Assign dedicated resources to social media response.
- Some organizations may choose to make social media their priority over regular media.
- Use social media as a dialogue, rather than press releases.
- Monitor social media to tailor external communications.
- Take advantage of Social Media Analytics (for example, this can provide you with a map of where the incidents are occurring nationally and globally).
- Maintain customer engagement on social media - especially for customer enquiries and concerns.
- Quickly prepare answers to media questions - get to the news makers before they get to you.
- Social media can make your stock price and reputation plummet.

Strategic Priorities During a Cyber Attack

During the exercise, participating cities were asked to provide their top five strategic priorities during a cyber-attack. The responses from each city have been summarized below, to be used as a reference when considering the priorities for your own organization:

Atlanta

1. Establish procedures based on roles.
2. What do you know? Keep adding to this. Don't underestimate the importance of social media and communication (internal and external).
3. Communicate and engage both internally and externally -- with transparent dialogue.
4. Play "what if" scenarios before it happens.
5. Risk management centered around financial and investor relations

London

1. New EU-GDPR related data protection preparedness (and ability to demonstrate this to regulators);
2. Organize response team with different disciplines; ensure that a leader has been appointed, and all members are trained and knowledge of in-situ principles and behavior assessed, particularly re: new EU GDPR strictures;
3. Quickly prepare messaging once attack has happened;
4. Engage Employees, customers, suppliers, etc. early on and stay in touch;
5. CEO oversees all out-bound communications.

Washington

1. Response governance - roles and responsibilities, decision-making authority
2. Maintaining public trust through external communication
3. Determining scope of damage
4. Legal and regulatory compliance
5. Process improvement/lessons learned

New York

1. Communication (internal & external)
2. Understand complete scope (impact analysis), incident response / mitigation
3. Recovery
4. Outreach to industry and government
5. Legal and regulatory requirements

Sydney

1. Assessment of impacts / situational awareness
   - Technology update (frequent updates)
   - Critical timelines (from Operations)
   - Impacts
   - Communications
   - Staff, customers, government, media
   - Business continuity plan / Disaster Recovery invocation
2. Contact with your bank regarding what's happening
3. Security - physical, branches, property, staff + Investigation (government / sector / internal)
4. Initiation of Incident Response Team to Evaluate, Contain, Respond to crisis.
5. Message development internally, consistent message to outward facing staff, proactively develop website and social media.

Major Challenges

The following themes were raised as major challenges faced during a cyber-attack incident:

- Not knowing how the public would respond.
- The importance of continued monitoring: a cyber incident could be a distraction for a larger incident.
- Exhaustion of teams during recovery efforts.
- How do you spend your resources? (this is a leadership / HR concern)
- Critical information may be in someone's head and not written down or documented.
- Potential for liquidity issues when you suspend trading. Government intervention may be required.
- Preparing for communications with different regions and with customers regarding the specifics of the problem.
- Assembling a rapid response team that includes all the essential disciplines.

The discussions also raised the following valuable points about the challenges of preparing for a cyber-attack incident:

- Many organizations are not ready to handle this type of situation.
- Organizations are starting to focus more on preparedness for cyber-attacks.
- There needs to be greater focus on what organizations need to do internally to handle these types of situations.
- Having a diverse and complete team is important. Being able to manage in a crisis without a key person may be a challenge. Continuity is critical and you will need more than one team.
- Auditing the organization's systems architecture (including redundancy) is a challenge.
- Having the necessary processes and procedures in place is essential. By the time an incident happens it is too late, and critical mistakes are far more likely to be made.
- Plans are living documents and need to be continually updated and improved.
- Organizations may need to make some changes (whether that be systems, processes, training) to make sure they are resilient to handling these types of cyber-related situations.
- Better preparedness can be a side-effect of effective systems design.
- Teams need to practice, including the CEO who may be in the lead during an incident of this type.
- Preparedness is improved by participating in exercises such as this one.

Learnings

The following were the key learnings from the exercise, as outlined by each participating city:

Washington DC

1. Bringing in subject matter experts / third-party support.
2. Details matter – organizations need to prepare for real life scenarios.
3. Rippling impacts can be significantly damaging.

New York

1. Must have a business continuity plan (internal).
2. Need to have a pre-planned strategic playbook.
3. Need for a collaborative environment - we are in this together.

London

1. Most of us are not adequately prepared.
2. Move quickly to isolate the problem.
3. Move quickly to communicate understanding of developments to stakeholders, honestly, realistically and with confidence.

a. Regularly review your media management plan to include any relevant changes.

Atlanta

1. Be ready and practice to adapt.
2. Exercise your plan.
3. More communication is needed pre-crisis; Understand the role and impact social media plays; Stay engaged; Address how larger companies can better support smaller companies with IR support.

Sydney

1. Design matters – having well designed systems and processes can help reduce the challenges and/or impacts associated with an event of this type. Systems should be architected upfront with resilience and redundancy in mind.
2. Importance of continually re-evaluating critical timelines during the incident, listening for regular updates from your tech experts.
3. Importance of clear communications with staff, customers and stakeholders, and having a consistent voice throughout all messaging.

The exercise ran for a duration of 90 minutes.

About the Organizers

SafeAmerica / WorldSafe

The SafeAmerica Foundation™ is a 501(c)(3) non-profit chartered in 1994, with headquarters in suburban Atlanta. The Foundation partners with corporate, governmental, public and private sector organizations, and other non-profits to save lives by emphasizing safety education and emergency preparedness.

WorldSafe is the International arm of the SafeAmerica organization, applying its charter and promoting safety education and emergency preparedness in other parts of the world.

For more information, see *www.safeamerica.org*

Avalias

Avalias Group Pty Ltd is a private company, based in Sydney Australia, specializing in software and services for emergency preparedness, business continuity and compliance. The company's scenario-based training and simulation technology, Avalanche TTX, was used to deliver this multi-city tabletop discussion exercise.

Avalias CEO, Harold Wolpert, acted as the Exercise Director and all software and services were donated on a voluntary basis. Avalias is a legally separate and independent entity.

For more information, see *www.avalias.com*

Disclaimer

The opinions expressed in this report are those of the exercise participants and do not necessarily reflect the views or recommendations of SafeAmerica/WorldSafe or Avalias.

This post-exercise report has been written in general terms and therefore should not be used as a substitute for creating robust plans and procedures for your organization. Application of the principles outlined in the report will depend on the circumstances of each specific situation. We therefore recommend that you obtain further professional advice before acting, or refraining from acting, on any of the contents of this publication. SafeAmerica/WorldSafe and Avalias accept no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

SafeAmerica/WorldSafe would be pleased to put readers in contact with experts who can assist with applying the principles set out in this publication to specific circumstances.

Report created by Avalias.