U.S. TRAVEL ASSOCIATION'S

SECURE TOURISM SUMMIT

KEY TAKEAWAYS

LONE WOLF ATTACKS EMERGE AS KEY CONCERN FOR SECURITY PROFESSIONALS.

In the past decade and a half, U.S. officials have become adept at identifying, responding to, and preventing large scale terrorist attacks on U.S. soil. However, the rise of lone wolf attacks is a key concern. These random attacks are often difficult to anticipate and detect. Security officials will need to focus their efforts on bolstering their defenses against these small-scale operations.

MUSCLE MEMORY: THE KEY TO SUCCESSFULLY IMPLEMENTING CRISIS PLANS.

Practicing a crisis plan sharpens your organization's response, helps anticipate new threats, and allows an organization to prepare for situations it might not have thought of or initially planned for. Simply put: it's not enough to develop a crisis plan – organizations and employees must frequently rehearse, adjust and re-evaluate.

CYBER-SECURITY MISNOMERS.

When it comes to protecting against cyber security intrusions, organizations often believe their cyber security leader must be the most technically sophisticated staffer. But resourcefulness is more important than high-tech savvy. The cyber security leader must be someone who can galvanize resources across departments and know who to coordinate with in the event of an emergency. And, given the threats facing companies today, many believe the best response is the most expensive cyber security technology available. But the fact is, merely covering the essentials can take 80 percent of the threat off the table.

MAINTAINING SECURITY AND PRESERVING THE CUSTOMER EXPERIENCE.

Bolstering security while also maintaining the customer experience is critically important. If an organization adds a new security procedure or protocol to their facilities, customers are likely to accept it, so long as it's not overly intrusive and the organization makes an effort to explain why it's necessary. At the same time, no single entity should be solely responsible for security at events. Everyone – businesses, law enforcement, private citizens – must play a role in the solution.

ALIGN YOUR MESSAGE WITH THE AUDIENCE'S SENTIMENTS.

Showing empathy for your audience and aligning messaging with their emotions is paramount. Moreover, delivering your message in simple, plain language is most effective. Above all, demonstrate authenticity and a commitment to transparency throughout the crisis – don't hide the truth and don't fail to answer hard, but essential, questions.

BIOMETRICS WILL SOON GIVE CONSUMERS MORE CHOICES WHEN INTERACTING WITH SECURITY TECHNOLOGIES.

The advent of programs like TSA PreCheck and Global Entry and the growing popularity of biometric technologies are revolutionizing security protocols at airports, stadiums, and other soft targets as well as changing the way we interact with cell phones and tablet devices. As biometrics become more common, the public will begin to be able to choose which biometrics they prefer to use – whether it's an iris scan, fingerprinting, or voice recognition technology. Many of these technologies already exist but there hasn't been enough consumer demand yet for them to be brought to market.

HELPFUL TIPS TO REMEMBER

CRISIS PLANNING AND READINESS

- **BRING THE OUTSIDE IN.** When developing a crisis plan, reach out to colleagues outside your department and immediate network. Most are going to be willing to provide input and feedback and share ideas that you might not have thought of.
- **DON'T WORK IN SILOS: GET TO KNOW LOCAL AND FEDERAL PARTNERS.** Include local, state and federal officials in crisis planning, regardless of how small an event is or how unlikely it may be that a crisis could occur. Build strong communications with officials, partner together to run crisis exercises and share your organization's expertise.
- **BUILD MUSCLE MEMORY.** Practice, practice, practice your crisis plans. It will sharpen your organization's response, help anticipate new threats, and force you to prepare for things you may not have thought of before.
- **BE PROACTIVE VS. REACTIVE.** Regularly schedule time to re-evaluate and adjust your crisis plans.

CYBER SECURITY

- **INTEGRATE CYBER SECURITY INTO YOUR ORGANIZATION'S OVERALL SECURITY STRATEGY.** It is no longer a matter of if – but when – an organization will be hacked. It is imperative that executives ensure cyber is a key component of their security protocols.
- **KEEP IT SIMPLE.** Some organization leaders are overwhelmed and unsure of how to properly prepare for cyber-attacks. But by just doing the essentials, an organization can take 80 percent of the threat off the table.
- **PRIORITIZE RESOURCEFULNESS ON YOUR CYBER SECURITY TEAM.** Your cyber security chief does not necessarily need to be the most technically savvy – but must be someone who can pull resources together and knows who to coordinate with.

CRISIS COMMUNICATIONS AND RAPID RESPONSE

- **BE AUTHENTIC AND TRANSPARENT.** Audiences respond best when you level with them. Explain the situation in clear, plain English and don't hide important information.
- **SHOW EMPATHY.** Align your message with your audience's emotions and point of view.
- **REMEMBER "THRDD".**

  TRUTH – Establish the ground truth.
  HOMEWORK – Do your homework before you talk to the press.
  REPORTER – Think like a reporter: what questions will you get?
  DEFINE – Define your message: what's your headline?
  DISCIPLINE – Stay on message.