# The New Prevention Movement

Why some of the biggest names in industry, homeland security and public safety are getting behind an effort to fundamentally alter how we think about safety and security.

**LiveSafe, Inc.**
1400 Key Blvd., Suite 100
Arlington, VA 22209

**(703) 436-2098**
contact@livesafemobile.com
www.livesafemobile.com

By Dan Verton
September 2018

# The Invitation

Smart people listen to Fred Smith and Barry Diller. And why wouldn't they?

In 1965, Smith predicted that the growth of the computer industry would spur the need for a faster and more reliable shipping service for spare parts. Today, FedEx is a $60 billion logistics company with 400,000 employees working in almost every corner of the world.

Diller, on the other hand, went from working in the mailroom of the William Morris Agency to pioneering the concept of the made-for-television movie and negotiating broadcast rights to major feature films. Today, the media executive who heads IAC and who has been the driving force behind major Internet brands, such as Expedia, Match.com, Tinder and The Daily Beast, has a net-worth of more than $3 billion.

So, when Fred Smith and Barry Diller say they think they've found a way to reduce the increasing number of risks and threats facing businesses while simultaneously improving safety and security for millions of people around the world, smart business leaders tend to stop what they're doing and listen.

"As CEOs we see ever increasing risks and threats to our businesses and our country – terrorist attacks, workplace violence, sexual assault, harassment, cyber threats, and many other types of safety and security incidents – resulting in human tragedy while costing our businesses and our nation billions of dollars annually," Smith and Diller wrote in a letter sent last August to 600 of the nation's largest corporations and institutions. "Something must be done to stem the tide. We think we've found a solution that changes the equation and moves us from reacting to incidents to preventing them."

They were tapping into an urgent need that all Fortune 1,000 CEOs and security officers share. U.S. companies spend more than $300 billion annually on legal fees, investigations and lost wages stemming from incidents of workplace violence, theft, injury and misconduct. And while most have established tip lines, toll-free telephone numbers and anonymous drop-boxes to collect tips from employees on emerging safety and security threats, the vast majority of post-incident investigations still uncover people who knew something that could have prevented the incident from happening but didn't report it.

"While all of us have made significant efforts to react and respond to incidents when they occur, there has been far too little emphasis placed on precluding problems from happening in the first place," Smith and Diller wrote. "Yet prevention provides a far greater return on investment than responding after the fact."

The two industry titans then urged the CEOs of America's leading businesses to send their chief security officers, human resources directors and chief legal advisors to one of five regional security

summits at which a new “game-changing solution” would be discussed. "The results have been outstanding – from substantial reductions in the costs of safety-related incidents to saving lives and keeping employees out of danger," they wrote.

# The New Prevention Movement

To the surprise of many of the Fortune 500 CEOs who received this letter, Smith and Diller were not the only big names on the signature line. Joining them in this effort to "quickly change the threat equation we all face" was Tom Ridge, the nation's first Secretary of the U.S. Department of Homeland Security, and Raymond Kelly, the legendary former Commissioner of the NYPD.


Kelly, a straight-talking former U.S. Marine who rose to prominence as the head of the nation's largest police department in New York City, had never endorsed a commercial product before. People who know Kelly said privately that his outright endorsement of the LiveSafe approach to community-based intelligence was a significant departure for the 43-year veteran of the NYPD. But the way Smith and Diller talked about it made it clear to him that this wasn't just another Silicon Valley marketing ploy. This was a movement.

"They see what I think of as the cornerstone of the new prevention movement," Kelly said, speaking in September at the first Re-Envisioning Security Summit in New York City. Fred Smith "believes the LiveSafe system is really a revolution in helping business identify risk," Kelly said. "He thinks it can significantly reduce litigation, injuries, crime, and ultimately terrorism, as it's sort of deployed throughout the world. He asked me to take a look at the system. I could not say no to Fred Smith."

> “I’ve never endorsed a product before or endorsed a movement. I'm endorsing a concept of calling for more focus on prevention and a sharing of information.”
>
> ➢ *Ray Kelly*
> *Vice Chairman of K2 Intelligence & former NYPD Commissioner*

# What Is Prevention?

At its core, prevention in the safety and security context is about detecting and disrupting potentially dangerous behaviors, activities or physical conditions before they escalate into a crisis. In the safety context, this could mean facility issues that pose risks of injury or bodily harm. In the security context, this often means detecting suspicious behaviors that could escalate to some form of violent act.

But the concept of prevention is also about people and culture. There is a tendency to view prevention as solely within the realm of stopping high-consequence, low-probability incidents (such as terrorist attacks and active shooters) from occurring. But the New Prevention Movement is really an approach to fundamentally change organizational culture from one of reaction to one of vigilance and shared responsibility.

To accomplish this, prevention must be built into the daily life of organizations and communities as they deal with the low-consequence, high-probability incidents that are commonplace (i.e. tripping/falling hazards, dangerous facility maintenance issues, intoxicated fans at stadiums and arenas, petty crimes and illegal contraband, or policies and procedures that cause bad customer experiences). The more we condition employees and community members to share the responsibility of reporting these issues (issues that have a direct impact on their working environments), the better prepared the organization/community will be to deal with those rare, major incidents that pose dangers to large numbers of people.

Given the human and cultural drivers that must be in place for prevention to succeed, prevention must be a business or organizational priority, driven from the top-down through policy and from the bottom-up through employee/community engagement. Whether intentional or not, the success of campus police chiefs and corporate chief security officers is too often measured in how well they react to incidents and manage crises rather than their ability to prevent incidents from happening in the first place.

The New Prevention Movement seeks to change this formula. Campus police chiefs and corporate CSOs must become cultural change agents and be given the appropriate discretionary budgets to enable them to test and experiment with new prevention concepts and technologies. But cultural change will only be possible with the direct cooperation and participation of other organizational and community leaders, including directors of human resources, facility managers, legal counsels, college and university presidents, as well as student and employee representatives.

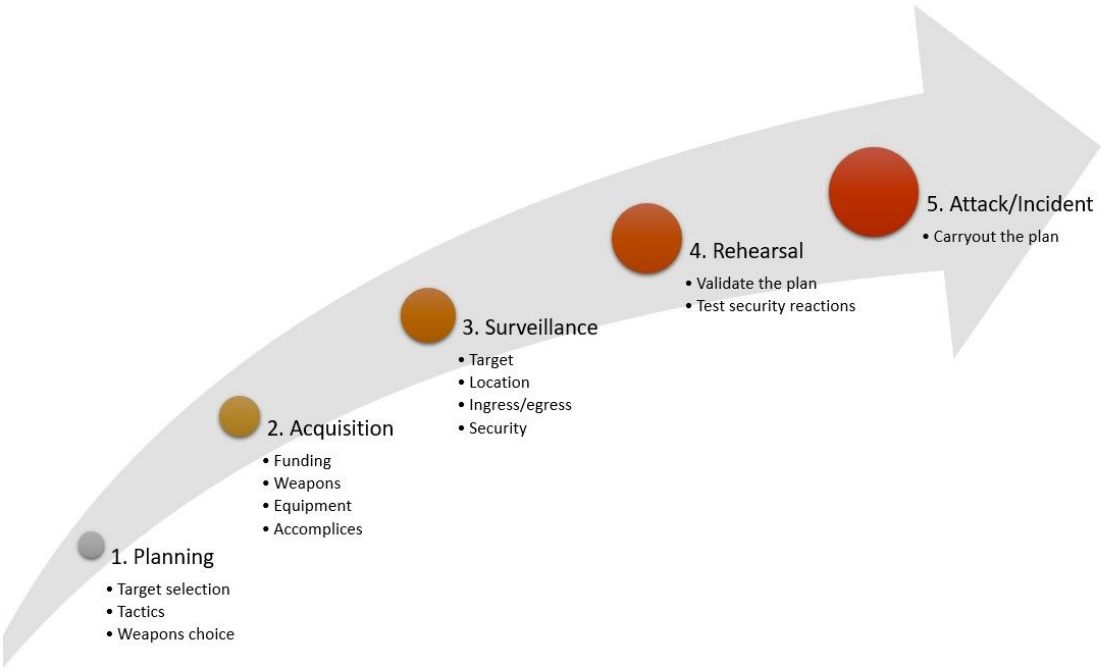
# Breaking The Cycle

Perpetrators of violent crimes, whether terrorists, sexual predators or mass shooters do not suddenly “snap” and carry out their acts. They plan their actions, sometimes meticulously down to the

last detail. Targeted acts of violence are often preceded by a series of stages, all of which are designed to improve the chances of the attack succeeding. This is critical to our understanding of prevention, because all of these pre-attack/pre-incident activities can be observed and reported by vigilant bystanders.

For example, consider the terrorist attack cycle in **Figure 1**. We know from more than a decade of studying major attacks that terrorist groups often follow a well-defined attack process that is observable at every stage. For a terrorist attack to succeed, the attackers must succeed at every stage. But observers can detect, report and break the attack cycle at any stage. And many attacks, known and unknown, have been averted because of somebody who saw something that looked suspicious and reported it.

**Figure 1: Terrorist Attack Cycle**

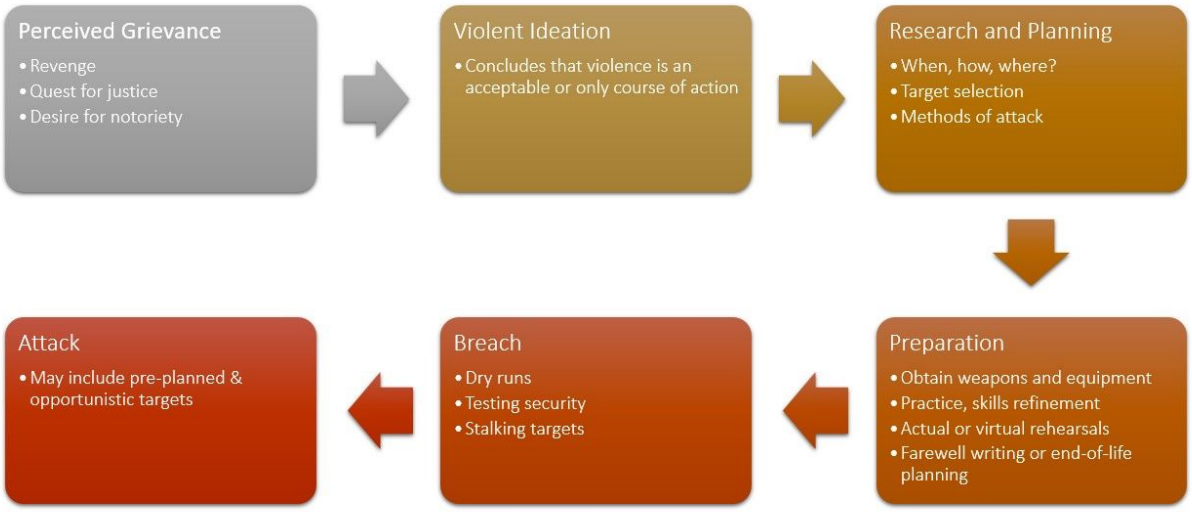



Taking what we know about the terrorist attack cycle, how might we think about targeted acts of violence, such as school shootings, mass murderers and sexual predators? **Figure 2** adapts the terrorist attack cycle to these other forms of violence that schools and businesses are defending against on a daily basis. These pathways to violence are based on years of study by the FBI's Behavioral Threat Assessment Center (BTAC).[1]

It is important to remember that, as with the terrorist attack cycle, pathways to violence can differ from one attacker to another and can overlap. Likewise, rehearsals or activities that look like dry runs can be the actual attack.

[1] "Making Prevention a Reality: Identifying, Assessing and Managing the Threat of Targeted Attacks." U.S. Department of Justice, Federal Bureau of Investigation, 2015.

**Figure 2: Pathways to Violence**




If we've learned anything from the recent spate of school shootings, it is that the vast majority of violent attackers exhibit warning behaviors throughout their individual pathways to violence that are often unusual and alarming to those who observe them.

These behaviors cannot predict violence, but for the diligent observer can help map a potential escalation to violence that should be reported to local security officials.

According to the FBI's BTAC, warning behaviors are dynamic and represent changes in patterns of behavior that may be evidence of increasing or accelerating risk. "When warning behaviors are evident, they require a threat management strategy and operational response. They are, for the most part, proximal behaviors, occurring more closely in time to a potential act of targeted violence," states a BTAC study.[2]

The BTAC study offers one important caveat, however: "For each 'successful' targeted violence offender with any given behavioral past, there are likely many more who exhibited similar behaviors, but never attacked. Warning behaviors cannot predict targeted violence, but are useful in identifying accelerating risk which should elevate concern."[3]

**Figure 3** details some of these potential warning behaviors.[4]

[2] Ibid., p. 32.
[3] Ibid.
[4] Ibid., pp. 33-36.

**Figure 3: Warning Behaviors**


# Why Prevention?

Kristina Anderson heard the first shots ring out around 9:40 AM on April 16, 2007. They sounded like they were getting closer and closer to her classroom. What may have seemed like an eternity was, in reality, only a few seconds. A gunman walked into her classroom at Virginia Tech in Blacksburg, Virginia, and began shooting.

Thirty-two people died and dozens were injured. Kristina was shot three times, but lived. She would be the most injured survivor of that horrible day.

As she healed during the weeks and months that followed, Kristina learned something that would change the course of her life: She would document at least 18 pre-attack indicators spanning several years that could have and should have led to greater scrutiny of the shooter's behaviors and mental stability leading up to the attack. They were indicators that should have been reported and should have prevented this tragedy from ever happening.[5]

According to Anderson, students commented on the shooter's odd behavior. For example, the shooter requested to be addressed as "question mark" in class, wore sunglasses while indoors, and took pictures of female classmates under

[5] Mass Shootings at Virginia Tech April 2007, Report of the Virginia Tech Review Panel.

tables. One former classmate recalled that his submitted writing assignments for an English class were deemed so "grotesque" and disturbing that they were not read in class. He was found "suspicious, creepy, or odd" among his peers.

Despite all of the warning signs, there was no easy way for members of the community to report their concerns to security or law enforcement. The dots in the Virginia Tech shooting went unconnected until it was too late.

"I was the only non-Virginian on the Virginia Tech panel," Ridge said, referring to the expert review panel established to study the circumstances and response surrounding the Virginia Tech shooting. "There were many signs prior to that horrific accident. If somebody would have been able to put a few of them together and maybe reach out to this young man and intervene at an earlier time, who knows what would have happened. But there was no chance because there was no way for people to aggregate that information and for someone to make a professional conclusion, we need some intervention here."

The same can be said for many other incidents in personal safety and security. From countering terrorism to sexual assault, harassment, suicide prevention, loss prevention in the retail sector, protecting lone workers, and collecting safety and incident intelligence throughout school campuses, arenas, malls and hospitals, employees are often aware of information that could prevent bad things from happening. But that information is of little use if it is not reported to the appropriate authorities.

Prevention is not a new concept. But scalable, enterprise-wide risk mitigation tools that are specifically designed and optimized for the human element to drive prevention are. By delivering technology that allows the human sensors that exist in every organization to light up with actionable security intelligence, organizations can alter the risk and security equation in their favor by driving prevention.


Businesses have spent billions of dollars aimed at managing risk and responding to workplace incidents of all sorts and sizes — including safety, security, sexual harassment, corporate malfeasance, and more. These costs, which can materially impact the financial well-being of a business, continue to skyrocket.

As is the case with coordinated terrorist attacks, the most serious security incidents rarely take place without revealing indicators that can be observed by people throughout the community. This is the key driver behind national programs like the "See Something, Say Something" campaign started in the

aftermath of 9/11 by New York's Metropolitan Transportation Authority and now promoted by the Department of Homeland Security.

Despite how much we know about pre-attack activities, reporting has historically been hampered by a multitude of human and technical factors. Employees are sometimes reluctant to get involved, particularly in cases of sexual assault. In many terrorism cases, observers of suspicious activities often don't report what they've witnessed out of fear of being accused of racial profiling. But even when employees do want to report something, they often don't know who to call and are further dissuaded by the lack of anonymity.

According to several industry executives who attended the Re-Imagining Security Summits, corporate toll-free tip numbers are overwhelmingly used for HR-related complaints. Very little information related to employee security and safety comes in through these traditional reporting channels.

"Ninety percent or more are complaints of an HR nature across our industry," said a senior executive from a major corporation in New York. "Somehow we're not getting as many [safety and security related reports] in the 800 numbers."

The New Prevention Movement, however, presents one of the best opportunities since 9/11 to significantly improve incident reporting. And with improved reporting comes an opportunity to leverage communities of interest for information sharing and threat triage across local, regional and industry boundaries.

# What's Changed?

If Smith, Diller, Ridge and Kelly are right, it is the ubiquity of the smartphone coupled with the cultural changes being ushered in by new generations of millennial and post-millennial college graduates that have made the new prevention movement possible.

"We believe technology has arrived at a point that enables fundamental change," Smith said. "Virtually everyone today has a smartphone, and everyone is comfortable using apps. These enable real-time communication and information sharing in ways that were never available in the past, and that enables the best source of safety and security intelligence, our employees, to communicate with our institutions."

"Ultimately, there's no better sensor than eyes on," said Ridge, speaking to attendees at the Chicago summit last October. "So many of the capabilities that you have are not connected to a mobile capability that you have on your person, all the time. You can have all the technology you want, but unless your people are empowered to help you keep that workplace safe you've missed the opportunity to do something very, very significant."

Fortunately, college campuses and corporate workplaces are also benefiting from generational changes in human behaviors. The availability of anonymous reporting has helped remove the stigma that has long been associated with calling out security and safety concerns in tight-knit communities, such as college campuses and corporate workplaces. In addition, younger generations of Americans have learned through tragedy to embrace the notion of community involvement and prevention.

According to the latest data from the Bureau of Labor Statistics, millennials (ages 22 to 37) and post-millennials (ages 17 to 21) make up 40 percent of the U.S. workforce.

"I think it's something we need to consider as we hire the new generation of workforce. They expect different ways to communicate," said an executive with a financial services firm in Dallas. "They don't communicate with us in the traditional ways of picking up the phone and calling us and that was the problem that we were facing."

"Five years ago you had the Millennials who were very comfortable, they did all self-provisioning, and now you've seen over the past three to five years just more universal adoption," said Carolyn Parent, president and CEO of LiveSafe. "People are very comfortable. There's not one of us sitting here today that doesn't have their phone either on their hip, in their pocket, or right in front of them."

> "We believe we must come together to build these communities. We need to change the equation from reacting to incidents, to preventing them."
>
> ➢ *Fred Smith*
> *Chairman and CEO, FedEx*

For large enterprises, the business case for prevention is getting easier and easier to make. It's not only about protecting employees, but it's also about the business benefits that come from prevention – the return on investment (ROI).

"I think the ROI is phenomenal," Ridge said at the Chicago summit, referring to the LiveSafe prevention model. "For a cup of coffee, you empower every single employee. If you think about empowering those employees in a world that's even more litigious, and the regulatory burden is even greater these days, to help them identify and avoid risk, you've done something very special, just within your corporate vertical."

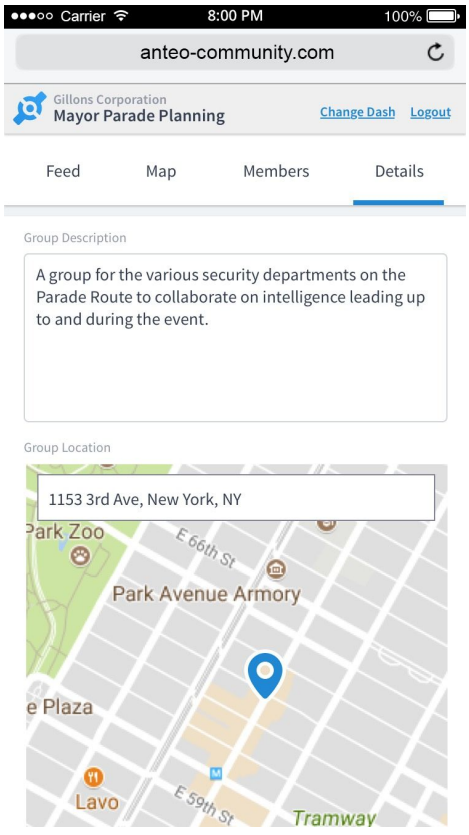
But the ultimate success of the new prevention movement will be measured in how well companies can share threat intelligence across organizational boundaries, according to Smith. "We believe we must come together to build these communities," he said, in a video message prepared for attendees at the Re-Envisioning Security Summit. "We need to change the equation from reacting to incidents, to preventing them."

"I think Fred and Barry's concept is to have this program proliferate, but also to enable companies to talk to each other in a more structured environment," Kelly said. "Their goal, as I understand it, is to promote this system, but enable it to get information and put it up into this structure where everyone can plug into it."

# Anteo

## See Something, Say Something ➥ Do Something

By the last Re-Imagining Security Summit in Atlanta, many of America's leading enterprises had come to an unsettling realization: their ability to collaborate and share risk intelligence at the local, regional and cross-industry levels was limited to group texts and emails.




Although security officials were making an effort to collaborate, such a haphazard approach to information sharing made it difficult, if not impossible, to ensure that warnings, tips and other observations could be acted upon in a timely manner. It also meant that the impact of local observations was limited to only those who were part of the group texts and email chain. Something more was needed – a force multiplier to make local observations and reports actionable on a broader scale to protect the broader community.

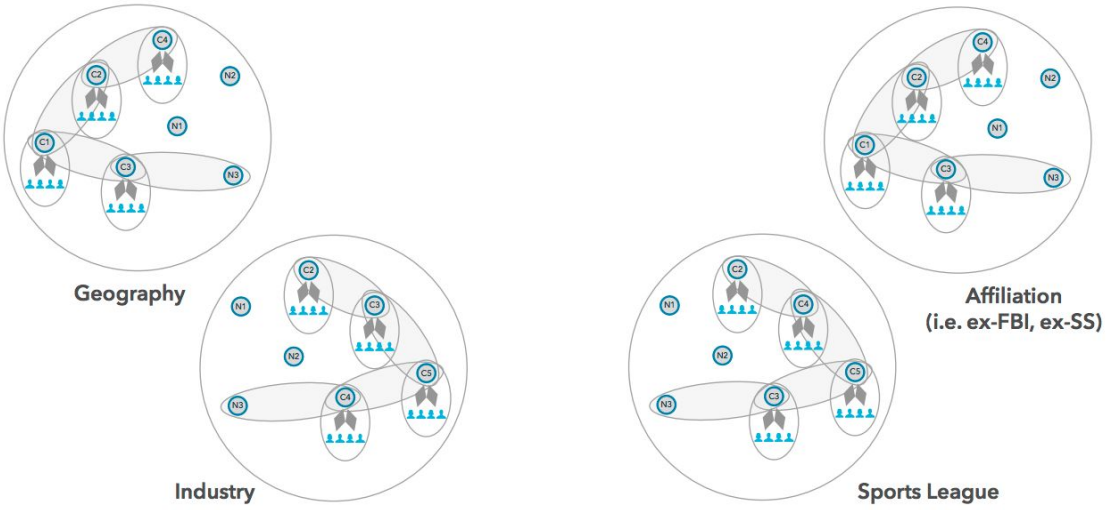
That was when LiveSafe customers and advisors saw the potential of leveraging the LiveSafe Mobile App to power dynamic and secure information sharing among chief security officers. And so was born the Anteo Private Security Community – the first-ever private, peer-to-peer security

community where trusted security and risk professionals from businesses and universities come together to share information and threat intelligence.

At the heart of Anteo is a community of trusted risk and security executives, who are known to one another and come together to dynamically form private security information exchanges. They share vetted risk and security insights, and in doing so exponentially drive quantity and quality of actionable security intelligence for the group. The value flows through the Community Collaboration Platform — a secure, shared channel for trusted collaboration, which is free to LiveSafe clients and non-LiveSafe clients, and requires no new hardware or software to deploy.

"We have significantly improved our ability to protect the employees and assets within our organizations. However, a threat or situation often also poses a risk to other organizations, either in the same area or industry," said Jim Cawley, Global Director of Corporate Security at Hearst. "The Anteo Community enhances our ability as security officials to collaborate by securely sharing specific threat or risk-related information, as well as insight, with a designated group outside of our own organizations. The use of this technology to enhance the corporate security community's situational awareness and share critical information with specific groups within the larger existing network of security professionals and peers outside of our organizations is a game-changer."

The dynamic creation of trusted groups within Anteo can be based around geography, industry, affiliation or other association. The Anteo Community gives each participant control over what information they share and who they share it with. This ensures that members are receiving information from a source that they know to be credible and relevant to their industry, event or location. Likewise, it ensures that important safety and security information is kept private and handled properly.




"Whether a situation occurs at the national, state or local level, security and law enforcement professionals have to rely on their integrated networks to gather as much information as possible, as quickly as they can," Ridge said. "The Anteo Community provides an opportunity to aggregate more

sources and provide timely and relevant information that helps someone, somewhere, someplace hopefully avoid the perils associated with that risk, whatever it might be."

"FedEx, IAC and many others in industry, universities, and other institutions are implementing this new technology now, and the benefits have been immediate and game changing." Fred Smith told attendees in his closing video remarks. "But the most serious incidents rarely happen in a bubble. Access to information from others increases situational awareness. Ultimately, the real value to our nation will be when we can share safety and security information among our corporate and other institutional communities. Crowdsourcing security information is the future, and we believe we must come together to build these communities. That is re-envisioning security."

## About The Author

Dan Verton is a homeland security and intelligence subject matter expert and content writer at LiveSafe. He earned a Master's Degree in Journalism and Public Affairs from American University in Washington, D.C.

Dan is a former intelligence officer in the United States Marine Corps and has consulted and produced security training programs for federal, state and local agencies. In one of his most recent roles, Dan served as an intelligence advisor to a nationwide federal terrorism awareness training program designed to teach tens of thousands of industry professionals how to identify and report terrorism-related suspicious activities.

He's written several books, including *Left of Boom: The Citizen's Guide to Detecting and Preventing Terrorist Attacks*, *The Hacker Diaries: Confessions of Teenage Hackers*, and *Black Ice: The Invisible Threat of Cyber-Terrorism*, and has testified before Congress twice on critical infrastructure protection.

## About LiveSafe

**LiveSafe was born from a spirit of triumph over tragedy.** Co-founders include Shy Pahlevani, a victim of a violent robbery, and Kristina Anderson, the most injured survivor of the 2007 Virginia Tech shooting.

The business they founded has grown into an award-winning innovative technology company that delivers risk intelligence solutions, safety communication infrastructure, and personal safety tools that power prevention for corporations and education clients. Organizations that have deployed the LiveSafe Solution include world-renowned universities, Fortune 500 media, financial services, and technology companies, commercial real estate powerhouses, malls, hospitals, stadiums, arenas, professional sports teams/leagues, and more.

www.livesafemobile.com @LiveSafe