WHITE PAPER
Insights for CSOs – October 2018

MAKING THE CASE

PREVENTION AS A STRATEGIC BUSINESS DRIVER

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

(571) 312-4645
contact@livesafemobile.com
www.livesafemobile.com

Teneo Risk
280 Park Ave, 4 th Floor
New York, NY 10017

(212) 886-1600
info@teneoholdings.com
www.teneoholdings.com

Making The Case:

Prevention As A Strategic Business Driver

Introduction

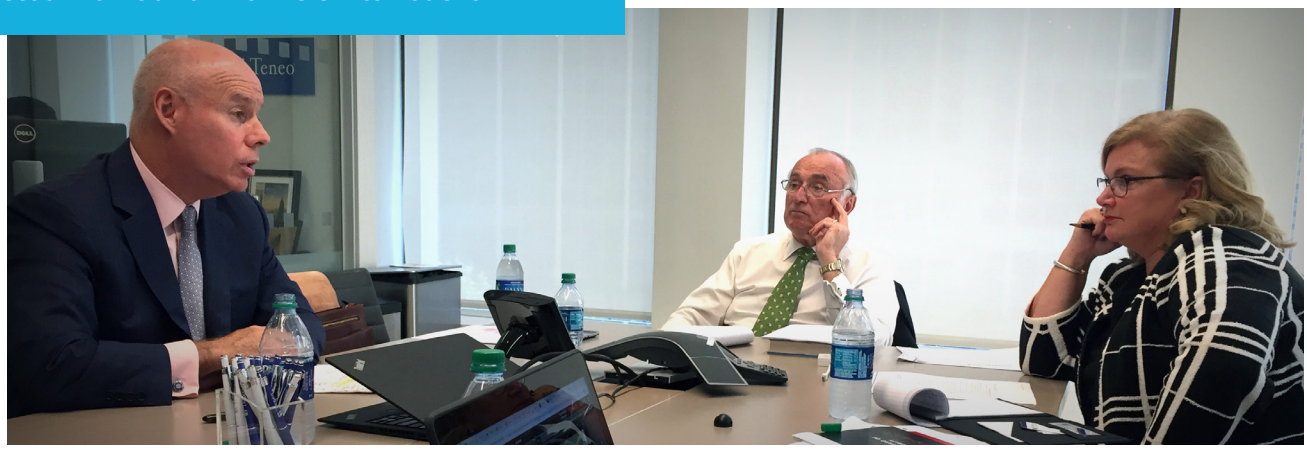
Whether it's the government or the private sector, Chief Security Officers are under immense pressure to justify their budgets, explain their policies and, in many cases, convince members of the C-suite and Board of Directors that they deserve a seat at the table.

Although effective security is no different from other corporate functions in terms of the need to demonstrate the return on investment to gain buy-in, communicating the value of security efforts can be a daunting task. Failures in security are loud and obvious to all. But success in the world of security usually goes unnoticed and unappreciated. The challenge for CSOs is to promote security as a strategic driver of business value and disprove the notion that security is simply a cost center that eats away at the bottom line.

This paper summarizes the key takeaways for CSOs looking to utilize a collaborative, data driven approach to demonstrating the ROI on security, as well as provides tips to cultivate a prevention mindset in today's complex and ever-changing world of risk mitigation and risk management.

Insights are derived from a live webinar hosted by ASIS International and featuring insights from Bill Bratton, the Executive Chairman of Teneo Risk and the former commissioner of both the Los Angeles and New York Police Departments; Pat Timlin, Chief Executive Officer of SilverSeal Corp. and the former Senior Vice President of Security and Life Safety at Brookfield Property Partners; and Carolyn Parent, the CEO and President of LiveSafe Inc., a growing company committed to helping business enterprises, universities and government agencies reduce their operational risk and prevent safety and security incidents from occurring.

Pat Timlin (left), Bill Bratton (center), and Carolyn Parent (right) host a live webinar with ASIS International



Prevention as a Strategic Business Driver

To date, the typical corporate C-Suite has been focused on strategies that prevent, mitigate, and manage security threats. But security is still often viewed as a cost or 'bottleneck' to doing business. As a result, security initiatives can sometimes be deprioritized, underfunded or miscommunicated, creating additional challenges for CSOs aiming to enhance an organization's risk posture.

> *"You have to be a leader. You cannot be passive. You have to have a vision for your organization that goes beyond just your area of responsibility."*
>
> **– Bill Bratton,**
> Exec. Chairman, Teneo Risk

A key part of overcoming this dilemma is ensuring that the investments in security and the corresponding benefits resonate with executive leadership in terms of value-add, return on investment and protection of people and assets. Although security professionals understand that security is not a cost center, changing that perception throughout the enterprise requires active leadership and necessitates outreach and influence with constituents.

"You have to be a leader," said Bratton. "You cannot be passive. You have to have a vision for your organization that goes beyond just your area of responsibility."

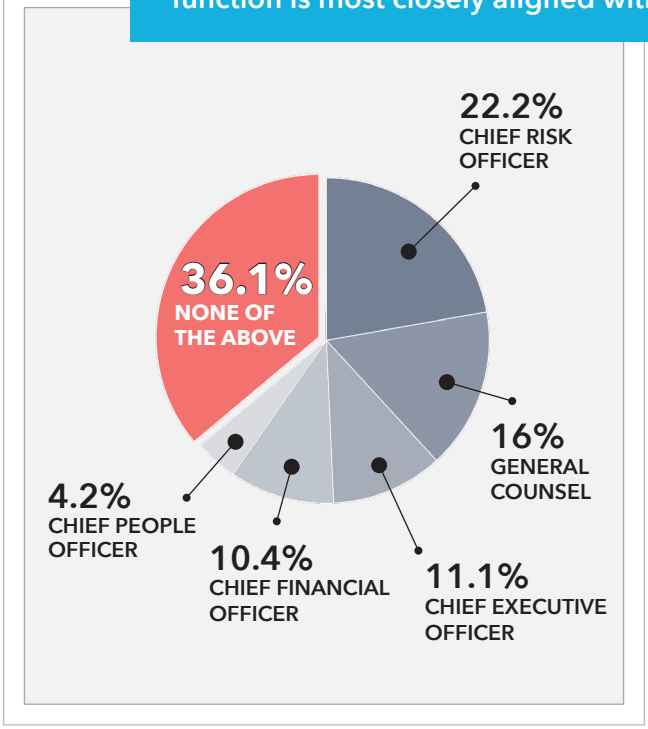
According to Bratton, CSOs must develop and sell a strategic vision of security that provides clear benefits for all lines of business. The multiplicity of responsibilities and threats CSOs face requires identifying and prioritizing synergies with the entire organization and the C-Suite.

"It starts with creating a platform – a plan or organizational structure that resonates with the organization's leadership so that you develop sponsors and collaboration," said Bratton. "You can't be reticent. You have to find a way to get yourself onto the leadership platform where you are noticed, respected and resourced properly."

However, when it comes to the tactical approach to selling security throughout the organization, "there are a lot of barriers to entry," said Timlin. "You have to position yourself for success. That is not a casual statement. It's important to have a structured strategic plan to get access."

So where do CSOs and other security professionals align within their organization? We posed that question to more than 320 webinar attendees in the security profession. And while 22 percent said they are most closely aligned with their organization's Chief Risk Officer, the responses show a wide variety of organizational structures at work. Bratton expressed dismay at the 36 percent who answered 'none of the above.'

SURVEY 1: "At my company, the Security function is most closely aligned with..."



"You've got to find a way to get into one of those five," said Bratton. "Because 'none of the above' is not going to get you anywhere." He also notes that you need to communicate your plans and recommendations using data and terminology these individuals like to and are used to consuming, whether in terms of benefits to your people with the head of HR or hard dollars to the head of finance.

> *"You've got to find a way to get into one of those five... Because 'none of the above' is not going to get you anywhere."*
>
> **– Bill Bratton,**
> Exec. Chairman, Teneo Risk

As part of that strategic plan, Timlin recommends that CSOs incorporate the risk issues that their company's Board of Directors cares about most – those risks that, if they occur, would potentially have significant operational or reputational impact.

The particular tactics or pathways by which the CSO chooses to sell the strategy can be daring or subtle, depending on the culture of the organization. "CSOs are engaged in every aspect of the corporation. War stories over coffee might get peoples' attention. Just make some friendships. Do some networking. It's not a one-person show," Timlin said. "Dial-in to the risk management and ROI nomenclature and people will pay attention."

Attaching ROI to Prevention

Proving a negative is a hard sell. That's why communicating the future cost savings through prevention of potentially costly incidents can be a monumental challenge for CSOs. But companies and industries have amassed mountains of data over the last several years detailing security incidents that have occurred and what those incidents have cost companies from both a monetary and operational perspective.

Leveraging stories about the damage other companies have endured because of lax security is what Timlin calls the "opportunistic marketing approach" to communicating security's ROI. But at the end of the day, hard data is even better, he says. "Intelligence-driven programs resonate with CEOs, Risk Officers and Boards of Directors," Timlin said.

"Intelligence programs are data driven. Bring data to the show. But the data needs to be meaningful and mapped to risks," he said. "I would price-out quite literally what would have prevented [an incident]. It's a very simple formula after you do that."

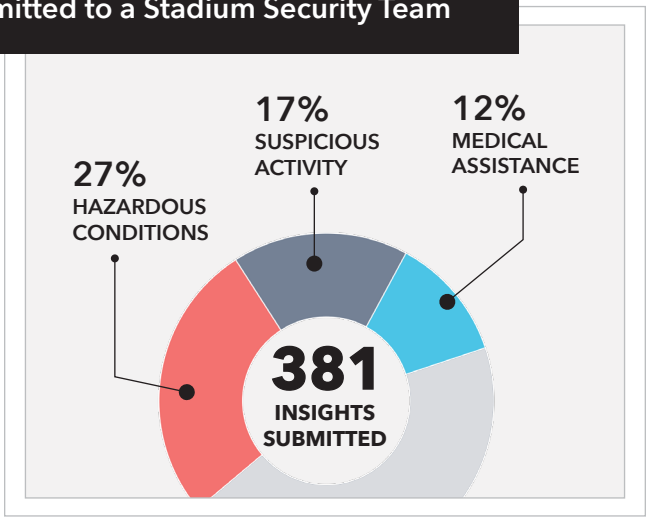
Recent analysis conducted by LiveSafe of prevention data collected from an anonymous stadium/arena organization shows that ROI can be communicated in specific dollar amounts.

Using a conservative pricing methodology, backed by research from consultancy Teneo Risk, LiveSafe found a client in stadium and arena management achieved a solid return on investment by purchasing the LiveSafe platform to crowdsource their threat intelligence. This was based on tying incident cost data to the types of reports surfaced over the course of three years.

> *"Intelligence programs are data driven. Bring data to the show. But the data needs to be meaningful and mapped to risks. I would price-out quite literally what would have prevented [an incident]."*
>
> **– Pat Timlin,**
> CEO, SilverSeal Corp.

The following charts outline the methodology, conservative cost data and likely savings based on an initial contract value of $75,000 for purchasing the LiveSafe platform to generate employee-sourced / community-sourced risk insights.

CHART 1: Overview of Insights Submitted to a Stadium Security Team



The 381 insights reported by LiveSafe users at this particular arena spanned a wide variety of risks, from suspicious persons and photography, to missing children, fans requiring first aid and broken glass in crowded public areas.

LiveSafe categorized the incidents from 1 to 5, based on severity, with level 1 being the least severe and level 5 being the most severe incidents. LiveSafe then based the ROI value on only level 4 and level 5 incidents, as outlined in Chart 2 to the right.

According to publicly available source data, the average settlement cost for incidents of workplace injury is approximately $20,000. Using this conservative cost estimate, we priced Level 5 incidents at $20,000 and the less severe Level 4 incidents at $5,000. Chart 3 (page 6) illustrates the way to calculate the bottom line ROI of preventing security incidents.

The methodology used in Chart 3 (page 6) requires additional explanation. Although all reports are valuable, not every report is a true incident. We should not assume that every tip/report received is related to a credible threat. There are many reasons that a tip may be a false positive (overstated risk by the reporter, duplicate report etc…). We removed those tips from the above analysis and conservatively decided to focus on a "hit rate" of 10 percent (1/10 tips) for the percentage of tips that would actually prevent a safety or security incident from occurring. In addition, incident pricing is based on open-source research conducted by Teneo Risk and uses the lower average cost per incident for workplace injury ($20,000). For the less severe (level 4) incidents – where significant harm is less likely, but additional costs like staff retraining, negative PR and customer loss are possible – we based the cost conservatively at 25 percent of the level 5 incident cost, or $5,000.

"When you go to the Chief Risk Officer, CFO, CEO or the Board, they absolutely know how much was paid in terms of insurance, investigations, and litigation," said Carolyn Parent, CEO and President of LiveSafe. "Attaching ROI to security can definitely empower the contribution of the CSO. If your leadership team isn't security minded, then speak in terms of ROI."

Bratton, however, cautioned CSOs to set goals without setting yourself up for failure. "Right-size the way forward. Set achievable goals related to your security plans which will benefit your stakeholders and demonstrate the value early and often delivered from your roadmap," he said. "And always try to be cost-effective. If you stay contemporary with the new technologies coming online, you can show how expenditures lead to long-term cost savings while enhancing the security posture."

CHART 2: Relative Value / Severity of Reports Sent To Stadium Security Team

SEVERITY	EXPLANATION	% OF TIPS RECEIVED
One	Fairly innocuous information, suggestion, or other	7%
Two	Information exchanges, contact supervisor, lost and found, visitor entrance	17%
Three	Unsecured infrastructure, repair needed, cleaning needed, traffic incident	36%
Four	Warning signs, danger possible, suspicious activity	18%
Five	Incidents occurred, high severity incident may occur, medical or security assistance, lost child	22%

CHART 3: The ROI Of Preventing The Most Serious Incidents

TIP SEVERITY	FIVE	FOUR
TOTAL # OF REPORTS RECEIVED	84 tips	69 tips
# OF PREVENTATIVE REPORTS RECEIVED	8	7
AVERAGE INCIDENT PRICE	$20K	$5K
COST TO COMPANY	$160K	$35K

RETURN ON A $75K CONTRACT = $195K

Cultivating a Prevention Mindset

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 actions or behaviors that could escalate to some form of violent act.

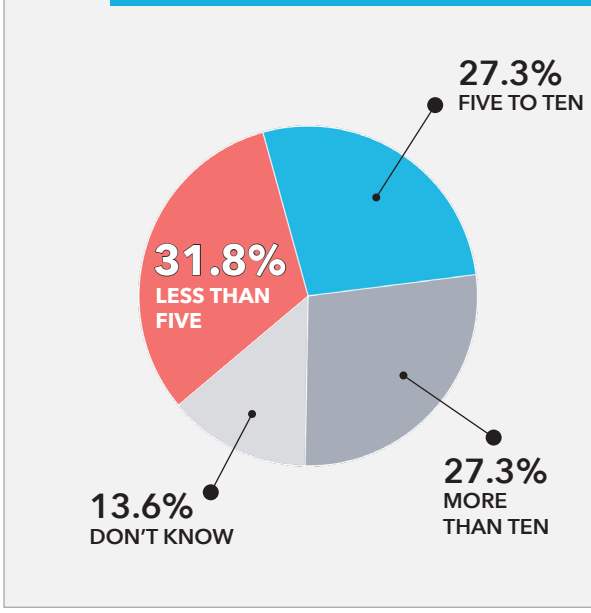
But the concept of prevention is also about people and culture. Prevention must be built into the daily life of organizations as they deal with the low-consequence, high-probability and commonplace incidents (i.e. workplace injury, dangerous facility maintenance issues, intoxicated fans, unattended bags, broken locks or lighting issues in parking lots). The more we encourage and incentivize employees and community members to share the responsibility of reporting issues that directly impact their working environments, the better prepared the organization will be to deal with those rare, major incidents that potentially endanger large numbers of people.

A survey of the webinar attendees revealed that companies are beginning to realize the value of employee/people-sourced risk intelligence, with nearly 55 percent receiving more than five people-sourced tips per month.

"Our experience has been if people can get comfortable with the technology and observing and reporting everyday common things, such as ice in the parking lot, a door that doesn't lock or an unattended package, then when the bigger issues come along like harassment or a physical security threat, they will be more comfortable using technology to report the risk," Parent said. "And the majority of the risks that can hurt you from an operational or reputational perspective," she added, "are known to some people in your organization."

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

SURVEY 2: "We all agree that human intelligence is the most valuable kind of intelligence. How many people-sourced tips do you get monthly?"



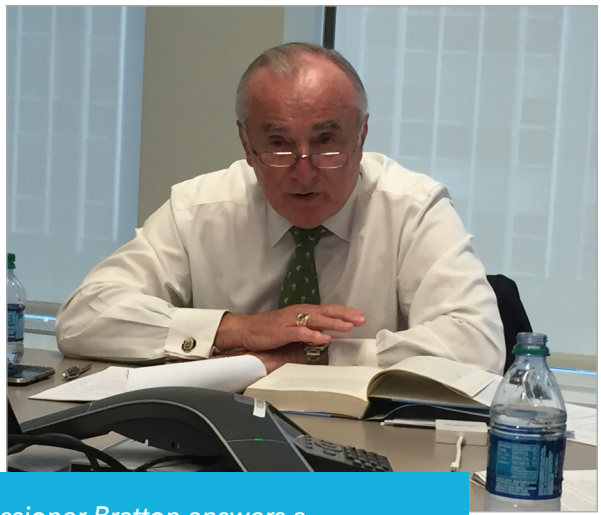
employees on emerging safety and security threats, the vast majority of post-incident investigations still uncover people who knew something that could have prevented the incident from happening but didn't report it.

Timlin agreed. "People tend to think of these incidents as acts of God. The sad truth is that most of these things are very predictable and preventable," he said.

The challenge, however, is devising an effective method for communicating and selling prevention across the organization. "That's a different approach than selling up [to the CEO or Board]," Timlin said. He recommended "packaging security as an amenity for your workforce, clients and tenants."

"The most important word in the security risk vocabulary is prevention. That's what it's all about."

– Bill Bratton,
Exec. Chairman, Teneo Risk



Commissioner Bratton answers a question for the webinar participants

Bratton agreed, comparing the goals of communicating prevention to the ultimate goal of the DHS 'See Something, Say Something' campaign. "What is See Something Say Something about? It's about inclusion," Bratton said. "Understand your workforce. How do they receive and interact with information? What is the concern of your employee base? People want to talk about quality of life - what they are experiencing every day," he said. "The most important word in the security risk vocabulary is prevention. That's what it's all about."

Pat Timlin comments on real-time poll results during the live ASIS webinar

"People tend to think of these incidents as acts of God. The sad truth is that most of these things are very predictable and preventable."

– Pat Timlin,
CEO, SilverSeal Corp.

About LiveSafe

LiveSafe helps organizations reduce operational risk by enabling them to prevent serious safety and security incidents using insights from their people. LiveSafe's risk intelligence technology platform consists of a Smartphone App and a Command Dashboard that are designed to enhance the situation awareness of security departments by delivering reports from employees and community members related to emerging safety and security risks and other malfeasance issues – and it does so while simultaneously protecting users' privacy and confidentiality by allowing anonymous reports.

The company has the support of major business leaders and public safety and security experts, including former U.S. Homeland Security Secretary Governor Tom Ridge, former Director of the U.S. Secret Service Mark Sullivan, former NYC Police Commissioner Ray Kelly, former Boston Police Commissioner Ed Davis, and more than 300 forward-thinking enterprises, universities, and organizations, including Hearst, IAC, Cox Communications, Brookfield Properties, the Consumer Technology Association, the San Francisco 49ers, and many more.

LiveSafe can be downloaded for free from the Google Play or iTunes app stores. Follow LiveSafe on Twitter @LiveSafe, and learn more at LiveSafeMobile.com.

About Teneo Risk

In today's complex operating environment, organizations are charged with mitigating an array of interdisciplinary and intersecting risks across the enterprise, whether terrorism, reputational risk, geopolitical risk or cyber threat. The complexity of this risk landscape demands new mitigation strategies and tactics that transcend traditional security processes.

Teneo Risk complements Teneo's comprehensive CEO advisory services platform, enabling a holistic approach to help clients address these issues within the context of their own unique operations.

Follow Teneo on LinkedIn, and learn more at teneoholdings.com.