



THE CSO CENTER
**FOR LEADERSHIP
& DEVELOPMENT**

ASIS International

12th Annual CSO Summit

WASHINGTON, DC

5-7 May 2019


CSO Influence: Adding Value Across the Enterprise

Executive Summary





Increase the value of security



The security industry has come a long way since pen-and-paper operations and guesswork decision-making. Today, the industry is waking up to technology and realizing how interpreting data and trends keeps environments safe and businesses running smoothly.

But the security landscape is constantly changing, and decision-makers are constantly searching for the best solutions. That's why we reshape our security workforce management software to fit the industry's current and future needs.

We're not only iterating our software though. We're also collaborating with security professionals and taking the conversation around security best practices forward through engaging content year-round. Check out Convergence - our quarterly eMagazine, Security Influencer Series interviews, blogs, whitepapers, and much more!

TRACKTIK

Contact us to achieve your vision of security

4200 Boulevard Saint Laurent #445
Montreal, QC, Canada, H2W 2R2
sales@tracktik.com
+1 (888) 454-5606



EXECUTIVE SUMMARY

CSO SUMMIT 2019

Are you relevant in a business environment bursting with new technology, changing demographics, and shifting roles and responsibilities, where every leader is expected to master key skills such as innovation and emotional intelligence? Members of the CSO Center for Leadership and Development community convened in Washington, D.C., on 5–7 May, at the 12th Annual CSO Summit to discuss and debate those and other game-changing issues. The Summit's presenters and attendees discussed issues ranging from the strategic to the tactical, centering around the theme of “CSO Influence: Adding Value Across the Enterprise.”

Sponsored by Global Guardian, Endera, LiveSafe, and TrackTik, the event kicked off with a welcome from ASIS International 2019 President Christina Duffey, CPP, who highlighted the new direction of ASIS International. CSO Center Advisory Council President Joe Olivarez, vice president of global security and resiliency for Jacobs, exercised his own influence throughout the event, encouraging CSOs to take a more active role in their professional development, crediting personal gains and realizations borne from his own efforts. Brian Reich, head of global security and investigations at TD Bank, emceed the program with humor and insight.

Attendees also enjoyed an exclusive after-hours networking reception at the National Law Enforcement Museum, which highlights American law enforcement stories with immersive exhibitions and interactive programs.

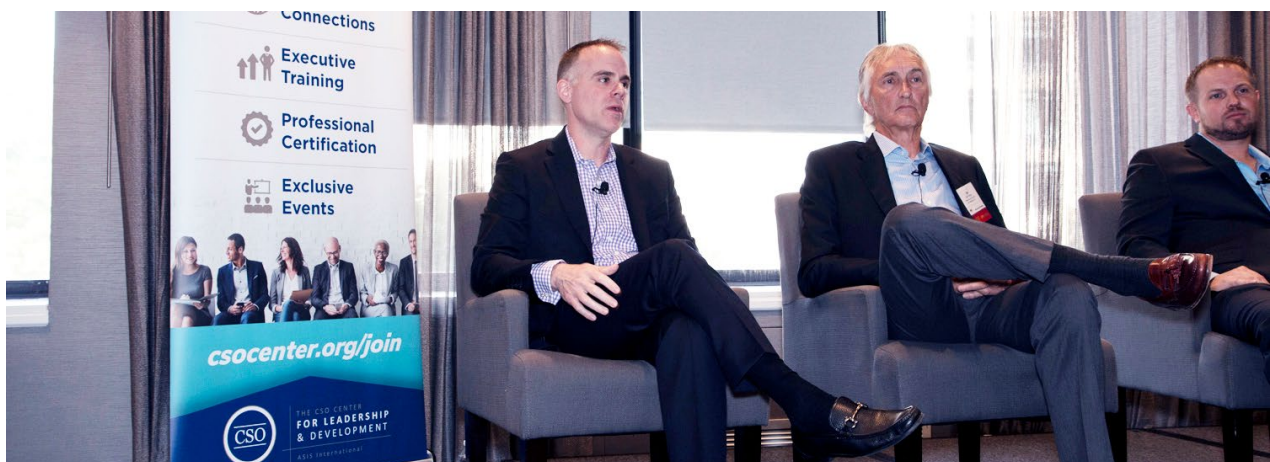
The event focused on the role of the CSO and the skills that lead to success, including understanding an organization's mission and value of other departments, overcoming assumptions with effective communications, and establishing a relationship with the C-suite and the overall organization in order to become a sought-after asset, capable of turning a company's vision into a secure and sustainable reality.

CSOs can continue learning how to develop these skillsets in the CSO track at 2019 Global Security Exchange (GSX) in Chicago, 8-12 September.



KEY TAKEAWAYS

- When security leaders can translate the language of risk, compliance, governance, and protection to other teams in an organization, they will find better outcomes and greater success.
- A new risk landscape is forming, with major power shifts, tectonic societal collisions, and bio-digital convergence expected to happen soon, in some cases as early as 2030.
- The many changes buffeting security are both creating new challenges and opening more opportunities for security professionals.
- Two- or four-year cybersecurity education is outdated. The new workforce needs training that can be done in months or weeks.
- To successfully integrate technology into a security team, you need to partner tools with the right users, such as analysts and intelligence experts.
- As the gig economy evolves, an organization may lose control over its brand or image, creating a new breed of challenges for CSOs.
- CSOs should be able to calculate and advertise the ROI that security can provide for the company's mission—focus on security's biggest priorities and where the money should go for the greatest impact.
- An innovative mindset, being willing to fail early and fast, and operating under a startup mentality can help create value and yield beneficial results for CSOs and their organizations.
- Establish yourself as a credible partner and do not pretend to be an expert on everything—instead, own your own process and learn or get help from others.
- CSOs need to develop relationships with others in the C-suite, along with establishing credibility and displaying confidence.



THE MEASURE OF CSO INFLUENCE

Not all leadership positions are created equal, said Andrew Donofrio, a certified coach, trainer, and former law enforcement officer. Executive level leadership in the security industry requires more than the typical C-suite skillset.

On top of the various security functions they must oversee and execute, CSOs must dedicate themselves to personal growth and leadership development. Such development should focus on the dimensions and challenges of CSO leadership; identifying and tackling top-level obstacles; and skills for success.

Working on the dimensions and challenges of leadership, CSOs should consider “Rainbow Leadership,” as their

role is replete with clashing views and judgment calls on how best to secure an organization. Rainbow Leadership is marked by establishing alignment with other departments, understanding the vision of the organization, and communicating effectively. Learning to speak the language of risk, compliance, and governance will lead to better outcomes because colleagues will see that you understand their perspectives and needs.

Leaders should also focus on honing their agility, which enables them to adapt and respond to various situations with greater success. These abilities correspond to leaders' other role: “You’re ultimately coaching and mentoring people on a regular basis,” Donofrio said.



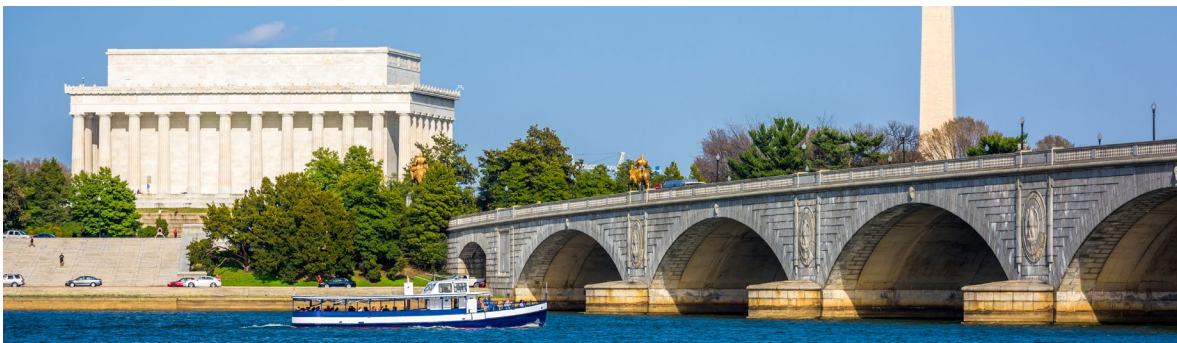
WHAT THE C-SUITE WANTS

A lively CSO Summit panel brought together C-suite leaders from multiple market sectors to discuss what they want and expect from their security leaders. Their advice boiled down to two key attributes: relationship-building and communication.

Security leaders should develop relationships with others in the C-suite, along with establishing credibility and displaying confidence. Part of that relationship involves working with partners to balance the often-competing interests of keeping a company secure while helping achieve its vision. When security leaders show they are actively involved in the company and its culture, it demonstrates that they not only understand, but care.

When CSOs talk to colleagues in different departments, they should be mindful of their communication style as well as the specific language they use. Using technical terms or jargon won't help their cause. CSOs should make security relatable to others in the C-suite, putting it into the context of the organization's mission. Members of the C-suite often don't understand the return on investment (ROI) that security can provide for the organization. It's security's role to make that crystal clear. When communicating, it is also useful to attach security priorities to larger corporate initiatives. Security benefits when its priorities are addressed in nonsecurity parts of the budget and when it can attach its initiatives to corporate ROI. Keeping language inclusive, rather than exclusive, also creates a positive influence, such as starting conversations with "we" instead of "I."

The C-suite wants an honest discussion with the security leader. Don't be afraid to educate your fellow executives on what they don't know about security, be part of the discussions, and take the initiative to understand the inner workings of your organization's operations.





INNOVATIVE SECURITY LEADERSHIP

Tomorrow's security professionals face a future environment of evolving technology, threat vectors, and culture that will impact strategy, structure, and processes. Grant Fisher, founder of PhnRe, and Masseh Tahiry of Toffler Associates led an interactive discussion about the future of security and CSOs as innovators. It included these key takeaways:

- Leaders should emphasize education, but not necessarily traditional four-year degrees. Cybersecurity programs, for example, should take months or even weeks—not two or four years.
- CSOs need to be innovators who understand how innovation can be an impactful force multiplier, helping security professionals create value as well as accomplish their own goals.
- Elevate security to be a strategy function.
 - When they partner with innovators, CSOs add value to their organizations.
 - Be willing to fail early and operate under a startup mentality, directing innovation or at least giving guidance to move things along quicker.

A CEO PERSPECTIVE ON SECURITY

“Risk management now has been elevated to a board imperative... It's become mission-critical,” said Mark Ein, CEO of Venturehouse Group, in an interview-style session with CSO Joe Olivarez, President, CSO Center Advisory Council. Ein, an entrepreneur who has been a fixture in the Washington, D.C., business scene for decades, spoke about how security at his various companies have benefited his bottom line.

When dealing with the C-suite and other executives, CSOs can shine when they show how security provides ROI. However, gains are not limited to a monetary value; CSOs can improve the business by providing insights into areas such as space utilization or increased efficiency. This has the potential to make a CSO a superstar.

Another way for a CSO to simultaneously add value and address a shifting landscape is by implementing technology effectively, using it to go from reactive to proactive. “It's such a game changer for everyone in the security industry,” Ein said, adding that innovation is ultimately about making security more effective and less intrusive.

SCENARIOS FOR CREATING INFLUENCE

In a session designed to encourage strategic collaboration, CSOs performed tabletop exercises about how they would respond to one of four scenarios: a terrorist threat coinciding with a Board of Directors site visit in Ukraine; a conflict between customer service and security in a financial institution with offices all over North America; a lucrative potential acquisition of a company in a country with high political, security, and compliance risks; and the prospect of decentralizing a corporate security department in a multinational conglomerate.

CSO Summit attendees shared strategies and methods of influencing stakeholders in the organization, including how to brief C-suite executives about potential risks and suggested actions, how to navigate legacy issues and change longstanding organization culture, and how to defend a corporate security program.

Consider this scenario: A multinational conglomerate that manufactures products, provides engineering services, and performs government contracting work is contemplating changing its operating model based on general and administrative expense concerns, changes in organizational structure, and board mandates. The corporate security function is currently centralized at the corporate office. One of the current board members works for a company that has security embedded in the business units, so is championing a change in structure. Further discussion has surfaced about the idea of moving all security responsibilities to the business units, which have minimal interaction with one another. The corporate office has approximately 1,500 employees globally; however, the remainder of the 75,000 employees are settled within the business units.



How would you go about defending a corporate security program vs pushing the mandate into the business units directly? Consider that you are looking into developing a GSOC and bringing travel under the security umbrella.

Attendees discussed this scenario and presented some thoughtful strategies:

- Engage the board member to understand the origin and context of the board member's quest to decentralize.
- Benchmark with other organizations that have undergone (or forgone) similar structural changes.
- Develop a business plan that outlines the pros and cons of a fully decentralized solution, a fully centralized solution, and a hybrid solution that can meet the needs of the unique divisions while keeping core functionality centralized.

**“YOU’VE GOT
TO PRACTICE
YOUR SECURITY
EVERY DAY.”**



TRAILBLAZER

In her more than two decades in law enforcement and security, the types of threats have not changed much, but the pace of threats has, according to Cathy Lanier, former Washington, D.C., Chief of Police and current CSO for the National Football League (NFL).

To keep up with threats to the enterprise, embrace technology and find the right staff, Lanier advised. Technology for its own sake is worthless; CSOs must match the people to the skills required by the new technology—meaning planning for new technology requires planning for its effective integration. For example, when implementing an integrated security technology system for Washington, D.C., Lanier knew that training lifelong homicide detectives to use the technology was unfeasible, so she hired a civilian team of tech-savvy analysts to support police officers and detectives and guide them through the system.

Drawing from her recent experience with Super Bowl LI in Houston and the 2019 NFL Draft in Nashville, Lanier said that matching people to the new technology isn't just about force multiplication. And it's not about risk management, which cannot stop a bad thing from happening, but can only mitigate how at-risk an organization is during certain events. While working for D.C., Lanier made sure to train and connect the right people to new technology, a partnership that assisted in lowering the homicide rate in the city by 90 percent.

When she moved to the NFL, Lanier said she had to learn how to influence stakeholders in the private sector, often negotiating with other NFL executives and partners at stadiums or cities to reach a mutually agreeable risk level.





ESRM IN ACTION

Enterprise Security Risk Management (ESRM) can offer CSOs a chance to partner with risk owners and work on becoming their enterprises' "influencer in chief." This panel discussion touched on the traits of strong ESRM programs, and what their leaders did to make them more successful:

- ESRM is not convergence; there are many ways to introduce ESRM without immediate wholesale adoption.
- Get a strategic plan in place and discuss it with leaders to better understand their goals—getting quick wins helps in building relationships and becoming a strategic and credible business partner.
- Be comfortable with saying "I don't know." Don't pretend to be a subject-matter expert on everything, just focus on owning the process of ESRM.
- Help the C-suite make early decisions that prove the value of security but be flexible because not everyone will inherently appreciate security. Find out:
 - Where you're at;
 - What you're starting with; and
 - How much pull you have.
- Go into a situation with an approach plan.
- Instill innovation in a way that works with your security culture.
- Recognize maturity factors of ESRM—what you can achieve for the business that results in bringing it closer to its goals.

The panel also used a real-time polling view to gauge the attendees' views on ESRM. Though few CSOs had a fully baked ESRM program, most had made solid progress, and virtually all considered the ESRM approach to represent the likely future of security.

THANK YOU TO OUR SPONSOR





BUILDING EXECUTIVE SUPPORT FOR INTELLIGENCE

Global security requires a global reach, and that requires a strong intelligence function, said Mike Hartnett of IHS Markit and Ed Pressman of TDI.

When taking an opportunities-entrepreneurial approach, CSOs should position the intel function to support the business more broadly, they said. Keep in mind major market shifts, strategy shifts, and corporate initiatives. The role of corporate security is to operate at the seams, and the opportunity to create business lies along those edges.

However, the C-suite sometimes has trouble recognizing the difference between intelligence and information. While information is simply raw, unfiltered data, intelligence is what makes a profit. Security executives can proactively position the intel function to support the business more broadly, acknowledging that better intelligence can help mitigate and

navigate risk, which is becoming more and more complex.

The challenge, they said, is in communicating the value of the intelligence function to the business. It would behoove CSOs to align themselves to give specific risk assessment and mitigation recommendations, instead of saying “yea” or “nay” to business initiatives, and to back up those recommendations with insightful intelligence that connects back to the business.

The panelists pointed to the future of security, recommending that CSOs start incorporating people with MBAs into their teams, bringing in younger generations of digital natives and data scientists, and perhaps even poaching financial experts from other parts of the organization to become intelligence analysts. Having these business-focused viewpoints can help to connect security’s intelligence to the organization’s success.

“YOU HAVE TO MATCH UP THE APPROPRIATE SKILLS TO THE TECHNOLOGY.”

THE CSO SUMMIT: AT-A-GLANCE

The following is a brief glance at the panels, speakers, keynote speakers, and facilitators at the CSO Summit.

DISCUSSIONS

What the C-suite Wants from the CSO: Panelists shared insight into the skills and relationships other C-suite executives want to see from CSOs, discussing and identifying the qualities and competencies that create effective collaborations and overcome an organization's challenges.

- Joanne Caruso, Chief Legal and Administration Officer, Jacobs
- Adrian Stanton, VP of Business Development & Community Relations, Virginia Hospital Center
- Richard White, Independent Consultant and Executive, Aerospace and Defense

What's Your Vision of the Future CSO? During this interactive session, discussion leaders and attendees debated current and future challenges to both a security team and its organization, with solutions for building a dynamic and resilient team, especially as public trust shifts.

- Grant Fisher, Founder, PhnRe Philosopher in Residence
- Maseh Tahiry, Risk Strategist, Toffler Associates

ESRM in Action: Identifying Levers of Influence and Vetting the Maturity Model: ASIS International's Michael Gips, CPP, Chief Global Knowledge Officer, moderated a panel on Enterprise Security Risk Management and how an effective program relies on collaboration and interaction between security risk managers and risk owners, with panelists discussing how security leaders can become an organization's influencer in chief.

- Toby Houchens, Founder/CEO, Alpha Recon
- William Phillips, CEO, New Source Security
- John Turey, CPP, VP, Enterprise Risk Management & Global Security, TE Connectivity

Table Exercises: CSOs Discuss Scenarios for Creating Influence

CSOs broke into groups to work through four unique exercises in influence: guiding the C-suite of an energy company through the potential threats to a Board of Directors site visit in Ukraine; exploring whether to decentralize a corporate security program; presenting the security risks

of a potentially profitable yet dicey acquisition in a high-risk country; and balancing conflicting security, culture, and customer service issues at a large financial services institution.

SECURITY SNAPSHOTS

Trailblazer: Cathy Lanier, former Washington, D.C., Chief of Police and current CSO for the NFL, discussed her experiences with risk management and security, leadership under crisis, and navigating security issues, especially for large organizations that are often in the spotlight.

The CSO of the Future: Caitlin Durkovich, Director of Toffler Associates, addressed large-scale technological advancements and shifts tomorrow's CSOs should be ready to encounter.

Change Agent: Bonnie Michelman, CPP, Executive Director of Police, Security, and Outside Services for Massachusetts General Hospital/Partners Healthcare explained how leaders can create influence and provide guidance for an organization during times of change.



SESSIONS

- **CSO Influence: Adding Value Across the Enterprise:** Andrew Donofrio discussed how executive level leadership in the security industry requires more than the typical C-suite skillset.
- **A Conversation with Mark Ein:** Mark Ein provided a CEO perspective on how security operates and can succeed in a changing business landscape.
- **Building Executive Support for the Intelligence Function:** The panel, consisting of Mike Hartnett, Director, Country Risk Consulting, IHS Markit, and Ed Pressman, Director of Intelligence & Strategic Advisory Programs, TDI illuminated the different perspectives on intelligence and data held by CSOs and other C-level executives, discussing how to best entice the C-suite into supporting intelligence programs.
- **Closing Keynote:** Stephen Laycock, Assistant Director, Directorate of Intelligence Division, FBI, spoke on how a relationship between government agencies and private enterprises can address challenges in the threat landscape and gaps in critical information.



THE CSO CENTER
**FOR LEADERSHIP
& DEVELOPMENT**

ASIS International

Questions?

Contact Carla Lochiatto, IOM, CAE, Director, CSO Center
Carla.Lochiatto@asisonline.org or +1.703.518.1500

Copyright © 2019 by ASIS International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

Printed in the United States of America

