C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

SPEAKERS



Abhay Shah
Head of Technology, Infosec Risk & Compliance
DoorDash



Richard Rushing
CISO
Motorola Mobility



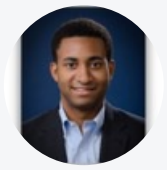
Katie Hanahan
Former Deputy CISO
Ingredion



Kenneth Townsend
Global CISO
Ingredion



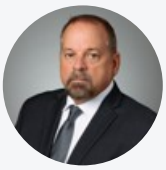
Nitin Raina
CISO
ThoughtWorks



Cole Sinkford
Global CISO
Globalfoundries



John Kellerhals
President / CISO
InfraGard Chicago



Philip Burnett
Information Security Officer
Navistar



Jeff Deakins
Director, IT Security (CISO) and Infrastructure
Marmon Holdings, Inc



Ralston Simmons
Director IS
Vivid Seats



Steve Rubinow
Associate Teaching Professor, College of Computing
Illinois Institute of Technology



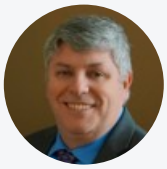
Jack Korzeniowski
Head of Cybersecurity & Risk
William Blair & Co.



Jeff Wolniakowski
CIO
Sage Equity Partners



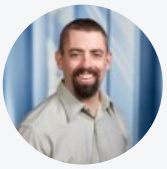
David Schaar
CISO / Director, IT Security & Compliance
Genuine Cable Group



Ken Kazinski
Global Cyber Security Management Attack Surface
Abbott



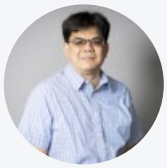
John Tryon
Deputy CISO
Health Care Service Corporation



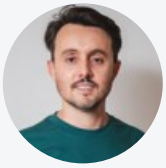
Brent Deterding
CISO
Afni, Inc.



Arun Desouza
Managing Director
Profortis Solutions



Eric Chantin
Director Center of Cybersecurity
Loyala University



Rogerio Godoy
CMO
senhasegura



Rahul Trivedi
VP of Operations
Executive Council for Leading Change (ECLC)



Grant Ecker
Founder, Chief Architect Forum. Former VP, Chief Enterprise Architect
Danaher



Fred Kwong
VP CISO
DeVry University



Casey Collins
Co-Founder
EliteOps



Grant Ecker
Founder
Chief Architect Network



Steve Rubinow
Professor & Director
Illinois Institute of Technology



Grant Ecker
Chief Architect / VP of Enterprise Architecture
ECOLAB

Click Here to Register

March 12, 2024

Central Time

Registration	**8:30 AM-9:00 AM**
Morning Networking	**9:00 AM-9:30 AM**
Opening Remarks	**9:30 AM-9:40 AM**

VISION VOICES KEYNOTE

Building a Cyber Resilient Culture

9:40 AM-10:05 AM

The ability of an organization to prepare for, respond to, and recover from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges.

In today's dynamic digital landscape, fostering a cyber-resilient culture is paramount. It involves not only fortifying defenses against current threats but also anticipating and preparing for tomorrow's uncertainties. To achieve this, organizations must prioritize both technical measures and cultivate a workforce that is informed, vigilant, and adept at responding effectively. This holistic approach extends beyond individual organizations, requiring collaborative efforts, information sharing, and awareness of emerging threat landscapes to create a network of resilience in the face of evolving cyber challenges.

SPEAKER



Kenneth Townsend
Global CISO
Ingredion

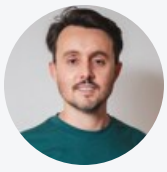
KEYNOTE

Securing Sovereignty: PAM Strategies in Defending South America's Supreme Court and Healthcare Giant Against Ransomware

10:10 AM-10:35 AM

In the dynamic landscape of cybersecurity, the imperative to swiftly rebound from adversities resonates deeply. As Rogerio De Godoy, Chief Marketing Officer at Senha Segura, articulates, organizations besieged by cyber adversaries must harness resilience and strategic defense to navigate threats effectively. Drawing from the compelling narrative of South America's distinguished supreme court and a prominent healthcare conglomerate, Rogerio illuminates how Privileged Access Management (PAM) became the linchpin in their resilience journey. Through proactive measures and decisive action, these institutions neutralized threats and fortified their defenses, emerging stronger post-attack. Rogerio's insights underscore the transformative power of PAM in safeguarding critical infrastructure, offering invaluable lessons for organizations striving to bolster cybersecurity resilience in an ever-evolving threat landscape.

SPEAKER



Rogerio Godoy
CMO
senhasegura

Coffee Break

10:35 AM-10:55 AM

PANEL

Gen AI - The Hype, The Story & Cybersecurity

10:55 AM-11:50 AM

GenAI, a revolutionary innovation in the world of artificial intelligence, has garnered immense attention and hype in recent years. Its story is one of rapid evolution and limitless potential, as it promises to transform industries, enhance decision-making processes, and revolutionize the way we interact with technology. However, amid the excitement, the role of cybersecurity becomes paramount. With GenAI's ever-expanding capabilities, the need for robust cybersecurity measures is essential to safeguard against potential risks and vulnerabilities. As we continue to unlock the possibilities of GenAI, the fusion of its incredible power with stringent cybersecurity practices will be the key to a safer and more promising future.

CHAIR



Grant Ecker
Founder, Chief Architect Forum. Former VP, Chief Enterprise Architect
Danaher

PANELISTS



Nitin Raina
CISO
ThoughtWorks



Rahul Trivedi
VP of Operations
Executive Council for Leading Change (ECLC)

DISRUPTOR

Hidden Market Inefficiencies In The Technology Ecosystem Inhibiting You From Growing Your Business and Reducing Risk

11:55 AM-12:10 PM

The expensive go-to-market motions of technology manufacturers and traditional partner ecosystems developed in the 1980s and 1990s have run their course. According to Gartner research, these outdated systems have contributed to 75% of B2B buyers preferring sales rep-free experiences from their suppliers. However, these rep-free experiences also lead to more buyer regret, underutilized software, and poor business outcomes. A better, more efficient model is needed to help today's digitally-minded companies continue to transform their businesses while dealing with increasingly complex threat and risk landscapes.

SPEAKER



Casey Collins
Co-Founder
EliteOps

Lunch

12:10 PM-1:10 PM

FIRESIDE CHAT

Third-Party Exposure

1:00 PM-1:35 PM

In today's interconnected business world, companies rely on vendors and suppliers for various services, which can pose significant cybersecurity risks. Third-party exposure is a major concern, as companies can be held liable for any data breaches or security incidents that occur due to the actions of their third-party providers. In 2024, this risk is expected to increase as companies continue to outsource work to third-party providers. This makes it more critical for companies to have effective security measures in place to properly secure third-party access. Failure to do so can result in data breaches, financial losses, and reputational damage. To mitigate this risk, companies must prioritize implementing comprehensive security measures that include vendor risk assessments, due diligence, contractual requirements, and ongoing monitoring. Additionally, companies must ensure that their third-party providers adhere to cybersecurity best practices and standards. By taking these proactive steps, companies can better protect themselves from the risks associated with third-party exposure in 2024 and beyond.

CHAIR

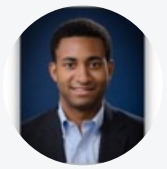


Arun Desouza
Managing Director
Profortis Solutions

SPEAKERS



Abhay Shah
Head of Technology, Infosec Risk & Compliance
DoorDash



Cole Sinkford
Global CISO
Globalfoundries

VISION VOICES

1:40 PM-1:55 PM

CyberSculpt: Crafting a Resilient Future - Navigating Cyber Culture and IT Security Maturity

Cybersecurity culture is essential in today's interconnected and technology-driven world to safeguard individuals, organizations, and societies from the rising threats in the digital landscape. A cybersecurity culture encourages proactive risk management, prompt reporting of potential threats, and adherence to best practices across departments by instilling a sense of shared ownership. When employees at all levels recognize their role in maintaining a secure environment, the organization becomes better equipped to detect, prevent, and respond to cyber threats effectively.
How do we measure our cultural maturity? As a CISO, how do we engage executive leadership teams to embrace and drive a security culture? Jeff will discuss different approaches and insights to engaging with the executive teams to improve security culture and drive a shared understanding of risks."

SPEAKER



Jeff Deakins
Director, IT Security (CISO) and Infrastructure
Marmon Holdings, Inc

VISION VOICES

2:00 PM-2:15 PM

Guarding the Cloud: Navigating the Rising Tide of Cloud Vulnerabilities and Cyber Threats in 2024

Cloud computing services have become a cornerstone of modern business operations, providing organizations with the agility and scalability needed to thrive in the digital age. However, in 2024, the threat of cloud vulnerabilities will continue to grow as more companies adopt cloud services. Cybercriminals are constantly finding new ways to exploit vulnerabilities in cloud infrastructure, which can result in data breaches, unauthorized access, and financial losses. To mitigate the risks of cloud-related security incidents, businesses must prioritize implementing robust security measures such as multi-factor authentication, encryption, and regular penetration testing. Additionally, businesses must develop comprehensive incident response plans that take into account the unique challenges of cloud-based attacks. By taking these steps, businesses can protect themselves and their customers from the growing threat of cloud vulnerabilities in the digital age.

SPEAKER



John Kellerhals
President / CISO
InfraGard Chicago

Networking Break

2:15 PM-2:35 PM

PANEL

2:35 PM-3:20 PM

CISO Mastery: The Nexus of Seamless Business-Technology Harmony

In 2024 the spotlight is on CISOs and their role in fostering this critical harmony. Emphasizing the need for both discipline and balance, CISOs are called upon to take ownership of challenges, acknowledging that when technology encounters failures, shared responsibility extends beyond individual roles.
Navigating the evolving landscape between business and technology demands a strategic blend of discipline and equilibrium, particularly as we enter 2024. Recognizing that, for many organizations, technology is the business itself, this session underscores the imperative of understanding technology as a critical enabler across all facets of the organization. From the front lines to the back office, technology serves as a potent tool for creating value by processing data, driving innovation, and challenging traditional business models.

CHAIR



Jeff Wolniakowski
CIO
Sage Equity Partners

PANELISTS



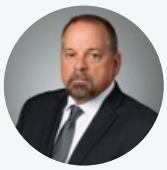
John Tryon
Deputy CISO
Health Care Service Corporation



Katie Hanahan
Former Deputy CISO
Ingredion



Fred Kwong
VP CISO
DeVry University



Philip Burnett
Information Security Officer
Navistar

VISION VOICES

3:25 PM-3:40 PM

Quantum Computing and IoT Security: A Dual Challenge for CISOs

As quantum computing edges closer to reality, organizations face a paradigm shift in cybersecurity. This session explores the potential impact of quantum computing on existing encryption methods, emphasizing the need for proactive measures by CISOs to fortify digital defenses. With the looming threat of quantum decryption rendering conventional security protocols vulnerable, CISOs must strategize for the post-quantum era. Simultaneously, the rapid proliferation of Internet of Things (IoT) devices amplifies the attack surface, intensifying the significance of robust IoT security. CISOs are tasked with safeguarding interconnected devices, data integrity, and user privacy. This abstract underscores the dual challenge of quantum computing's transformative potential and the imperative for enhanced IoT security, urging CISOs to spearhead adaptive strategies that secure organizations in this evolving digital landscape.

SPEAKER



Richard Rushing
CISO
Motorola Mobility

PANEL

Ransomware and Cyber Readiness

3:45 PM-4:30 PM

Ransomware attacks are in the headlines, affecting businesses and individuals in all sectors. Through 2024, these attacks have continued to grow, resulting in significant financial losses, data theft, and reputational damage. Even businesses that have achieved a level of cybersecurity compliance remain at risk unless they have understood what impact a ransomware attack really means in the context of their business.

The good news? When you have identified how to protect your business from a ransomware attack you have already defined what needs to be done to reduce your total cyber risk exposure across all levels of attack. Ransomware might be the most reported attack, but is nowhere near the most expensive or damaging cyber attack you might face.

CHAIR



Steve Rubinow
Associate Teaching Professor, College of Computing
Illinois Institute of Technology

PANELISTS



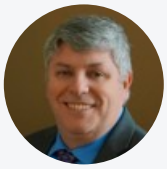
Ralston Simmons
Director IS
Vivid Seats



David Schaar
CISO / Director, IT Security & Compliance
Genuine Cable Group



Eric Chantin
Director Center of Cybersecurity
Loyala University



Ken Kazinski
Global Cyber Security Management Attack Surface
Abbott

Closing Remarks & Raffle Giveaway

4:30 PM-4:40 PM

Cocktail Reception

4:40 PM-5:30 PM

TOGETHER WITH

eliteops FORTRA™ senhasegura HCLTech OASIS Cribl CybelAngel Axonius Chi Networks™ CORO