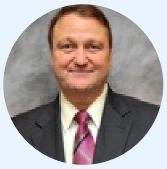
C VISION INTERNATIONAL

AGENDA

The Future of IT & Cybersecurity

CIO & CISO Ohio Think Tank

SPEAKERS



Alan Greenslade
COO
Fairfield Medical Center

Shawn Sines
CIO/CTO
Colgate 12

Paul Barnes
CTO
Installed Building Products

Kingshuk Choudhury
Chief Enterprise Architect
Cardinal Health

John Bruggeman
Chief Information Security Officer
CBTS

Rich Nagle
Deputy CISO
The Ohio State University

Michael Gross
Manager, Cybersecurity Intelligence
Cleveland Clinic

Click Here to Register

June 25, 2024

Eastern Time

Registration 8:30 AM-9:00 AM

www.cvisionintl.com

Morning Networking

9:00 AM-9:30 AM

Opening Remarks

9:30 AM-9:40 AM

KEYNOTE PANEL

CIO and CISO Nexus: Mastering the Art of Business-Technology Harmony

9:40 AM-10:25 AM

Bridging the gap between business and technology is not easy and requires discipline and balance between technology, people, and the business. For so many organizations today, technology is the business. Technology needs to be understood as a critical enabler in every part of the organization from the front line to the back office. It creates new value by crunching data to deliver new insights, it spurs innovation, and it disrupts traditional business models.
For business and technology leaders alike, new actions and behavioral changes can help their organizations make this shift. CIOs must take responsibility for problems, they should convey that when technology fails, many people typically share responsibility.

VISION VOICES KEYNOTE

Building a Cyber Resilient Culture

10:30 AM-10:45 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.

Coffee Break

10:45 AM-11:05 AM

KEYNOTE

Power of GenAI: Unlocking Innovation in the Cloud

11:05 AM-11:30 AM

This session will explore the convergence of cloud computing and generative artificial intelligence (GenAI) technologies, offering technology executives insights into the transformative potential of this synergistic relationship. From accelerating innovation and enhancing productivity to enabling personalized experiences and driving competitive advantage, GenAI-powered solutions in the cloud are reshaping industries and revolutionizing business operations. Join us as we discuss practical strategies and use cases for harnessing the power of GenAI in the cloud, including machine learning, natural language processing, and computer vision applications. Whether you're leading a technology organization or driving digital transformation initiatives, this session provides valuable perspectives on leveraging GenAI to unlock innovation and drive business success in the cloud-centric era.

PANEL

Gen AI - The Hype, The Story & Cybersecurity

11:35 AM-12:20 PM

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.

Lunch & Networking

12:20 PM-1:20 PM

PANEL

Strategic Shifts: Reimagining Engineering Talent Deployment and Management in the Age of GenAI

1:20 PM-2:05 PM

Unlock insights into the evolving landscape of talent deployment and retention as board expectations drive CIOs to rethink traditional IT talent models. Explore the impact of GenAI on coding processes and the software engineering lifecycle, and discover strategies for optimizing talent allocation and headcounts. Gain actionable insights into defining new roles, cultivating essential skills, and charting GenAI-centric career paths to align with organizational goals and stay ahead in a rapidly changing technological landscape.

FIRESIDE CHAT

Navigating Cybersecurity Risks in the Third-Party Ecosystem

2:10 PM-2:45 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.

DISRUPTOR

Quantum Computing and IoT Security: A Dual Challenge for CISOs

2:50 PM-3:05 PM

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.

Networking Break

3:05 PM-3:25 PM

VISION VOICES

Infinite Horizons: Unleashing the Potential of Generative AI in Shaping Future

3:25 PM-3:40 PM

Let's explore the transformative power of generative AI technologies and their profound impact on the strategic vision of CIOs. This keynote delves into innovative applications of generative AI, ranging from creative content generation to advanced problem-solving, providing CIOs with insights on how to leverage these technologies to enhance operational efficiency, foster innovation, and navigate the evolving digital landscape. Attendees will gain a deep understanding of generative AI's potential, empowering them to drive their organizations towards a future where limitless possibilities meet strategic IT excellence.

FIRESIDE CHAT

Decrypting Ransomware: Understanding Risks, Strengthening Defenses, and Securing Your Cyber Future

3:45 PM-4:20 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.

Closing Remarks & Raffle Giveaway

4:20 PM-4:30 PM

Cocktail Networking

4:30 PM-5:30 PM

PARTNERS

We are currently accepting partnership opportunities for this event.