C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

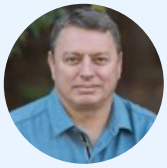
SPEAKERS

Cassie Crossley
VP, Supply Chain Security, Cybersecurity & Product Security Office
Schneider Electric

Dennis Barnes
VP Security and Infrastructure
San Francisco Fire Credit Union

Hemam Muthyala
Chief Security Officer
SPAN.IO

Akshay Wattal
Head of Security Engineering & Operations
Ripple

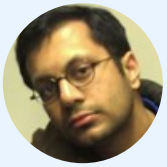


Chris Kirschke
Product Owner, GenAI Security
Albertsons Companies

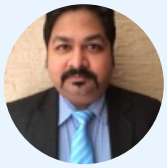
Steve Zalewski
Former CISO
Levi Strauss & Co.

Shadaab Kanwal
Managing Director Digital, Data and Analytics Services
Charles Schwab

Stephen Chen
CTO
Nucompass Mobility



Pratik Savla
Chief of Staff, Enterprise Security & Compliance
Synaptics Incorporated



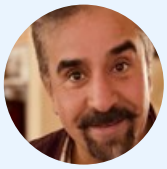
Anand Dutta
Global Head Solutions CoE, Presales & Alliance – Cybersecurity & Risk Management Practice
Tech Mahindra

Alex Derafshan
Head of IT and InfoSec
Lunar Energy

Srinivas Haridas
Head of Data Engineering
BMO Financial Group

Alex Marzano
CIO
NexGen Power System

Anand Thangaraju
Head of GRC Director Product Risk & GRC
Early Warning Services



Tas Jalali
CISO
AC Transit

Click Here to Register

June 04, 2024

Pacific 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

Cyber Security Evolution of Artificial Intelligence (AI): Friend or Foe?

9:40 AM-10:05 AM

The potential of Artificial Intelligence (AI) is vast, as it is now being utilized across all industries. With the combination of machine learning, AI has made significant improvements in the field of cybersecurity. Automated security systems, natural language processing, face detection, and automatic threat detection are some examples of how AI is revolutionizing cybersecurity. However, AI is also being used to create intelligent malware and attacks, which can bypass the most up-to-date security protocols, making it a double-edged sword. On the positive side, AI-enabled threat detection systems have the ability to predict new attacks and immediately notify administrators in case of a data breach.

KEYNOTE

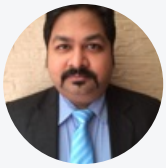
Building Cyber Fortitude: CISO Strategies for Resilient Cybersecurity

10:10 AM-10:35 AM

In the realm of building cyber resilience, organizations confront increased risk exposure amidst bold moves and evolving external challenges. Despite investments in technology and data, risk leaders, including CISOs, express difficulty in keeping pace with the persistent threat of cyber crises. However, in today's business landscape, discussions of digital transformation or reinvention are inseparable from considerations of cybersecurity. Looking ahead, stakeholders, from the board to frontline cybersecurity operations, pose critical questions about resiliency. This includes inquiries about the adequacy of efforts to safeguard the company and its customers

in the face of cyber attacks. The focus shifts to identifying opportunities to minimize the impact on business and shareholder value through effective threat response. Embracing cybersecurity as a whole-of-business endeavor, organizations are urged to align themselves with business owners, adapting to changes in the cyber landscape and fortifying resilience against disruptions. Building confidence in the cybersecurity program becomes paramount in navigating the dynamic and challenging cyber landscape effectively.

PANELISTS



Anand Dutta
Global Head Solutions CoE, Presales & Alliance – Cybersecurity & Risk Management Practice
Tech Mahindra

Coffee Break

10:35 AM-10:55 AM

VISION VOICES

Insider Threats

10:55 AM-11:10 AM

Despite advancements in technology, human error remains one of the most significant causes of data breaches. Whether it's due to a bad day or intentional misconduct, a single vulnerability can lead to the theft of millions of pieces of sensitive information and even jeopardize an entire organization. According to a report by Verizon on data breaches, approximately 34 percent of all attacks can be directly or indirectly attributed to employees. Therefore, it is crucial to create a culture of awareness within the organization to safeguard data in every way possible. This involves educating employees on data security best practices and implementing stringent measures to prevent insider threats. By taking a proactive approach to data protection, organizations can mitigate risks and safeguard their reputation while maintaining the trust of their stakeholders.

PANELISTS

Cassie Crossley
VP, Supply Chain Security, Cybersecurity & Product Security Office
Schneider Electric

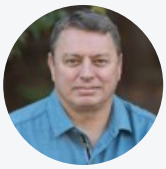
PANEL

Gen AI - The Hype, The Story & Cybersecurity

11:15 AM-12:00 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.

PANELISTS



Chris Kirschke
Product Owner, GenAI Security
Albertsons Companies

Dennis Barnes
VP Security and Infrastructure
San Francisco Fire Credit Union

Alex Derafshan
Head of IT and InfoSec
Lunar Energy

Lunch & Networking

12:00 PM-1:00 PM

DISRUPTOR

Fortifying Cyber Security Together: A CISO's Call to Increase Cyber Transparency

1:00 PM-1:15 PM

In the evolving landscape of cybersecurity, the imperative to increase transparency takes center stage, driven by new laws and regulations mandating prompt reporting of cyber breaches. A notable example is the SEC's cyber disclosure rule, necessitating companies to report incidents within 72 hours. This shift from voluntary to mandatory information-sharing not only presents challenges but also opportunities. Compliance empowers organizations to construct more comprehensive defenses and actions against cyber risks. Regulatory guardrails provide confidence, allowing companies to explore, experiment, and compete securely. To stay ahead, a tech-enabled approach embedding cybersecurity across the enterprise is crucial. Looking forward, collaboration with the C-suite, particularly the Chief Risk Officer and General Counsel, is vital. Crafting a consistent narrative, setting priorities, and adapting to new cyber risk management practices become essential. Moreover, understanding board expectations, simplifying complex cyber regulations, and extending cybersecurity measures to external reporting teams are key considerations for navigating the regulatory landscape effectively.

PANEL

Data Empowerment: A CISO's Guide to Unlocking Strategic Value Safely

1:20 PM-2:05 PM

CISOs are challenged to redefine their role not only as guardians of security but also as enablers of responsible and innovative data utilization. This directive emphasizes the importance of striking a balance between data protection and leveraging the full potential of organizational data assets. CISOs must collaborate with stakeholders to establish robust data governance frameworks, ensuring compliance with privacy regulations while facilitating the ethical and strategic use of data. By unlocking the value of data, CISOs contribute to the organization's competitiveness, innovation, and overall digital transformation. This session explores strategies for CISOs to harness the power of data responsibly, thereby positioning cybersecurity as an integral driver of business success in the data-

driven era.

PANELISTS

Alex Marzano
CIO
NexGen Power System

Srinivas Haridas
Head of Data Engineering
BMO Financial Group

VISION VOICES

2:10 PM-2:25 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.

PANELISTS

Anand Thangaraju
Head of GRC Director
Product Risk & GRC
Early Warning Services

Networking Break

2:25 PM-2:45 PM

DISRUPTOR

2:45 PM-3:00 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.

VISION VOICES

Cyber Hygiene 2024: Building a Secure Future in the Digital Era

3:05 PM-3:20 PM

In the digital age, practicing good cyber hygiene is essential to maintaining the security and integrity of personal and business data. However, in 2024, the lack of basic cyber hygiene practices will continue to be a major cause of cyber incidents. Cybercriminals exploit these vulnerabilities to gain unauthorized access to sensitive information, steal data, and launch damaging cyber-attacks. It's crucial for individuals and businesses to prioritize basic cyber hygiene practices, such as using strong passwords, regularly updating software, and backing up data. Additionally, individuals and businesses must educate themselves and their employees on cybersecurity best practices and the latest threats to stay ahead of the evolving threat landscape. By taking these proactive steps, individuals and businesses can protect themselves from cybercriminals who prey on poor cyber hygiene practices.

FIRESIDE CHAT

Ransomware and Cyber Readiness

3:25 PM-4:00 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.

PANELISTS

Hemam Muthyala
Chief Security Officer
SPAN.IO

Closing Remarks & Raffle Giveaway

4:00 PM-4:10 PM

Cocktail Networking

4:10 PM-5:30 PM

IN PARTNERSHIP WITH

FORTRA™ COLORTOKENS

Microsoft | TECH mahindra