C VISION INTERNATIONAL

AGENDA

The Future of IT & Cybersecurity

CIO & CISO Think Tank

SPEAKERS

Hans Vargas-Silva
Data Protection Lead- Cybersecurity Governance
Marathon Petroleum Corporation

Genaro Liriano
Director Technology Operations Risk Management
CIBC

Iain Paterson
CISO
WELL Health Technologies Corp.

Travis Walker
Senior Associate Information Governance, Privacy & Cybersecurity
Norton Rose Fulbright

Rob Knoblauch
Deputy CISO & VP Global Security Services
Scotiabank

Alfred Yau
Head of Global Banking Credit & Lending IT Canada
HSBC

Olya Sanakoev
CTO
Rogers Bank

Mamta Sethi
CIO - Group Functions Technology
Manulife Financial

Clive Williams
Head of Business Information Systems
Plan Group

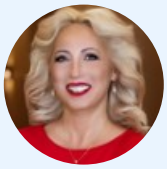
Simon Nuss
Vice President, Data & Analytics
Hitachi

Shane Coleman
VP, Solutions Engineering
Cyera US Inc.

Wayne Silberman
Field Technical Director - Canada
Cohesity

Luis Santos
CIAM Specialist
Okta

Tim Lam
Associate Partner and Project Director, Information Technology and OT and Telecommunications
CIMA+ Construction



Jenny Alfandary
Professor
University of Guelph-Humber

Click Here to Register

October 12, 2023

Eastern Time

Registration

9:30 AM-10:00 AM

Morning Networking

10:00 AM-10:30 AM

Opening Remarks

10:30 AM-10:35 AM

Generative AI Attack

10:40 AM-10:55 AM

The emergence of generative AI technologies has introduced a new and complex dimension to the cybersecurity landscape, presenting a significant challenge for CISOs, CIOs, and businesses at large. Generative AI can be weaponized by malicious actors to craft sophisticated and convincing cyberattacks, such as deepfake phishing emails or AI-generated malware. These attacks have the potential to deceive even the most vigilant users and traditional security systems, posing a substantial threat to data integrity, confidentiality, and overall business continuity. Consequently, CISOs and CIOs must adapt their cybersecurity strategies to incorporate AI-powered threat detection and mitigation tools while keeping abreast of the evolving tactics of adversaries. Furthermore, businesses need to invest in robust employee training programs to educate their workforce about the risks associated with generative AI attacks and foster a culture of cyber-awareness, ultimately safeguarding their digital assets and reputation in an increasingly AI-driven world.

PANELISTS

Rob Knoblauch
Deputy CISO & VP
Global Security
Services
Scotiabank

VISION KEYNOTE PANEL

Bridging the Gap Between IS/IT and the Business

11:00 AM-11:45 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.

CHAIR

Hans Vargas-Silva
Data Protection Lead- Cybersecurity Governance
Marathon Petroleum Corporation

PANELISTS

Alfred Yau
Head of Global Banking Credit & Lending IT Canada
HSBC

Olya Sanakoev
CTO
Rogers Bank

Mamta Sethi
CIO - Group Functions Technology
Manulife Financial

Building & Retaining The Team

11:50 AM-12:05 PM

Attracting and retaining team members depends in large part on understanding what drives employee job satisfaction. Many have seen declines in enterprise production and stakeholder satisfaction with the enterprise that track back to loss of key employees. Now is the time to confirm that your business is doing the right things to support the retention of highly valued talent. Effective leaders play an important role in the success of a business—and the success of the business' employees. There are a few reasons why effective business leaders are so important to their teams

PANELISTS

Clive Williams
Head of Business Information Systems
Plan Group

Lunch & Networking

12:00 PM-1:00 PM

DISRUPTOR

Building a High Confidence Cyber Recovery Plan

1:00 PM-1:15 PM

Data is a differentiator in the digital economy. That's why data has simultaneously become the most valuable and the most targeted business asset. Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion USD annually by 2025 and that companies will fall victim to a ransomware attack every 2 seconds by 2031. We have seen plenty of bad things happen due to insufficient security measures. As a species, we tend to wait for those truly significant "black swan" events before making substantial changes.
Move from waiting to anticipating, preventing and being cyber resilient. Hear from Cohesity as they will speak to some learnings on what C-levels of large organizations deal with and how you can learn to respond more effectively and strategically.

PANELISTS

Wayne Silberman
Field Technical Director - Canada
Cohesity

The Promising Future of Artificial Intelligence (AI): Opportunities and Challenges Ahead

1:20 PM-1:40 PM

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.

PANELISTS

Genaro Liriano
Director Technology Operations Risk Management
CIBC

Iain Paterson
CISO
WELL Health Technologies Corp.

DISRUPTOR

Your Most Important Asset: Data - Is It Really Secure?

1:45 PM-2:00 PM

Boosting data security posture is a top priority for organizations in 2023 and beyond. In a recent Forrester Research study commissioned by Cyera, 71% of security leaders said legacy technologies and manual processes inhibit business success. Join this deep dive discussion on why today's security executive expects the most transformational business benefits to come from automating data security, specifically risk assessments, data discovery, and classification.

Session topics will include:

The struggle to meet security goals while enabling the business to use data and advanced technologies
New approaches to data security that keep pace in the era of cloud and AI
Generative AI - risk versus reward

Embracing automation and rapid time are critical capabilities in cybersecurity

PANELISTS

Shane Coleman
VP, Solutions Engineering
Cyera US Inc.

Networking Break

2:00 PM-2:20 PM

PANEL

Digital Transformation Managing Data and Analytics

2:25 PM-3:10 PM

CIOs play a crucial role in driving their organization's digital transformation efforts. The COVID-19 pandemic has accelerated the adoption of digital technologies, and CIOs must continue to lead the way to stay competitive and meet the evolving needs of customers and employees. This requires a deep understanding of the organization's goals, processes, and IT infrastructure, as well as collaboration with other business leaders. By successfully leading digital transformation, CIOs can position their company for long-term success in a digital world.

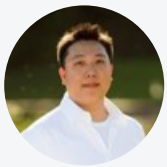
Data management and analytics are critical areas for CIOs to focus on as organizations continue to generate large volumes of data. CIOs must implement effective data management strategies to ensure that data is accurate, secure, and easily accessible. This involves developing processes for collecting, storing, and analyzing data, as well as ensuring compliance with data privacy regulations. Additionally, CIOs must leverage analytics to gain insights from this data and inform decision-making. By using advanced analytics tools and techniques, CIOs can identify trends, patterns, and opportunities that can drive business growth and enhance the customer experience. Overall, effective data management and analytics are essential for CIOs to help their organizations make data-driven decisions and stay ahead of the competition.

CHAIR

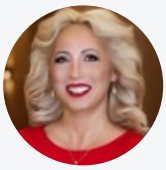
Hans Vargas-Silva
Data Protection Lead- Cybersecurity Governance
Marathon Petroleum Corporation

PANELISTS

Simon Nuss
Vice President, Data & Analytics
Hitachi



Tim Lam
Associate Partner and Project Director, Information Technology and OT and Telecommunications
CIMA+ Construction



Jenny Alfandary
Professor
University of Guelph-Humber

DISRUPTOR

Achieving the Perfect Balance: Customer-Centric Journeys and Identity Security

3:15 PM-3:30 PM

In the realm of identity security, the pursuit of exceptional customer experiences while maintaining top-notch security is a paramount challenge. We will delve into the crucial intersection of customer-centric journeys and security.

During this session, we explore prevailing industry trends and imminent threats, shedding light on the delicate equilibrium required to excel in the digital landscape. Dive into the world of identity security, gain insights into the contemporary landscape, and discover how the Okta Customer Identity Cloud can accelerate and boost revenues and empower organizations to swiftly navigate this complex terrain. Be equipped not only to strike the right balance today but also to thrive and prepare for the challenges of tomorrow.

PANELISTS

Luis Santos
CIAM Specialist
Okta

FIRESIDE CHAT
Cloud Computing & Vulnerabilities

3:35 PM-4:10 PM

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 2023, 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.

CHAIR

Iain Paterson
CISO
WELL Health Technologies Corp.

PANELISTS

Travis Walker
Senior Associate
Information Governance, Privacy & Cybersecurity
Norton Rose Fulbright

Clive Williams
Head of Business Information Systems
Plan Group

Closing Remarks & Raffle Giveaway

4:10 PM-4:15 PM

Cocktail Hour

4:15 PM-5:15 PM

TOGETHER WITH

okta LOGICGATE reco COHESITY aws