C VISION INTERNATIONAL

# AGENDA

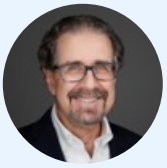
## Future of Cybersecurity

# CISO Summit

## SPEAKERS

**Octavia Howell**
CISO
Equifax Canada

**Shaun Khalfan**
SVP & CISO
Discover Financial Services



**Pasquale Cirullo**
VP IT
Richards Manufacturing Company

**Amresh Mathur**
SVP IT
Citizens Financial Group

**Devon Bryan**
Global CIO
Carnival Corporation

**Michael Orozco**
Managing Director
MorganFranklin

**Matthew Martin**
Former CISO
LPL Financial

**Michael Calderin**
CISO
YAGEO Corporation

**Shaun Marion**
Former VP & CISO
McDonald's

**Gal Tal-Hochberg**
Group CTO
Team8

**Laura Deaner**
CISO
Northwestern Mutual

**Nick Sims**
CIO of Neuromodulation
Fortune 500 Company

**Richard Rushing**
CISO
Motorola Mobility Inc

**Erik Hart**
CISO
Cushman & Wakefield

**Ketan Pandit**
Group CTO
QBE Insurance

**Gleb Reznik**
Managing Director
JPMorgan Chase

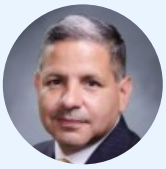
**Ivan Durbak**
CIO
Bronx Lebanon Hospital Center

**Arvin Bansal**
CISO
Fortune 500 Company

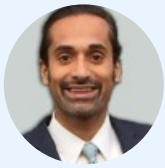
**Rick Patterson**
EVP CISO
Clear

**Allison Miller**
CISO & SVP
Optum

**Afzal Khan**
CISO
Opko Health



**Peter Rosario**
CISO
USI Insurance



**Sajed Naseem**
CISO
New Jersey Judiciary

**Damon Becknel**
CISO
ID.me

**Kelly Moan**
CISO
City of New York

**Olga Chaplygina**
Regional CMO
Ceasars Entertainment

**Ponnarasi Raj**
VP Technology Programs
BNY Mellon

**Chris Manteria**
CTO
Coldwell Banker American Heritage

**Edmond Mack**
Deputy CISO & VP Global Security Services
Haleon

**Click Here to Register**

## November 16, 2023

Eastern Time

## Welcome & Registration

9:30 AM-10:00 AM

## Morning Networking

10:00 AM-10:30 AM

## Opening Remarks

10:30 AM-10:40 AM

PANEL

## Social Engineering: New in 2023

10:40 AM-11:25 AM

Social engineering attacks are a growing concern for businesses and individuals alike, as cybercriminals continue to use advanced techniques to trick people into divulging sensitive information or performing actions that can lead to data breaches. In 2023, these attacks are expected to become even more sophisticated, making it increasingly challenging for individuals and businesses to identify and

prevent them. To protect themselves, individuals and businesses must be vigilant and aware of these tactics. They must also implement comprehensive security measures, such as security awareness training, anti-phishing software, two-factor authentication, and access controls. Additionally, businesses must establish policies and procedures for responding to social engineering attacks, including incident response plans, data backup and recovery, and regular security assessments. By taking these proactive steps, businesses and individuals can better protect themselves from the risks associated with social engineering attacks in 2023 and beyond.

**PANELISTS**

**Shaun Khalfan**
SVP & CISO
Discover Financial Services

**Arvin Bansal**
CISO
Fortune 500 Company

**Damon Becknel**
CISO
ID.me

**KEYNOTE**

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

**11:30 AM-11:55 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.

**PANELISTS**

**Devon Bryan**
Global CIO
Carnival Corporation

## Networking Lunch

**12:00 PM-1:00 PM**

**PANEL**

## Cloud Vulnerabilities

**1:00 PM-1:45 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.

**PANELISTS**

**Amresh Mathur**
SVP IT
Citizens Financial Group

**Afzal Khan**
CISO
Opko Health

## FIRESIDE CHAT
## Ransomware

**1:50 PM-2:25 PM**

Ransomware attacks are becoming increasingly prevalent and sophisticated, affecting businesses and individuals in all sectors. In 2023, these attacks are expected to continue to grow, resulting in significant financial losses, data theft, and reputational damage. Businesses should implement comprehensive security measures, including regular backups, employee training, and endpoint security, to minimize the risk of a ransomware attack. Additionally, it's important to have a response plan in place to minimize the impact of an attack if it does occur.

**PANELISTS**

**Octavia Howell**
CISO
Equifax Canada

## Networking Break

**2:25 PM-2:45 PM**

## PANEL
## Data Management and Analytics

**2:45 PM-3:30 PM**

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.

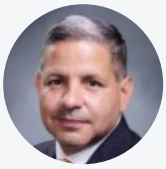
DISRUPTOR

## Insider Threats

3:35 PM-3:50 PM

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



**Peter Rosario**
CISO
USI Insurance

## Networking Break

3:50 PM-4:10 PM

DISRUPTOR

## Enhancing Security in Digital Transformation

4:10 PM-4:30 PM

In the realm of digital transformation, CIOs hold a pivotal and security-centric role, closely collaborating with the Chief Information Security Officer (CISO) to drive their organization's digital evolution securely. Accelerated by the COVID-19 pandemic, the adoption of digital technologies necessitates CIOs' unwavering focus on security to maintain competitiveness and meet the evolving needs of customers and employees while mitigating risks. By deeply understanding the organization's goals, processes, and IT infrastructure, and working in tandem with the CISO, CIOs establish a comprehensive security framework, emphasizing a security-first mindset, robust data protection, network security, cloud security, incident response, business continuity, risk-based approaches, and staying updated with security trends. Through this collaboration, CIOs position their company for long-term success in a digitally transformed world, ensuring a secure and resilient digital future.

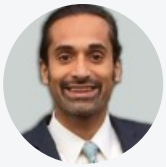
PANEL

## The Growing Importance of Cybersecurity for CIOs in 2023

4:35 PM-5:20 PM

In 2023, the threat of cyber attacks continues to grow, making cybersecurity a top priority for CIOs who must take proactive measures to ensure that their organization's information systems and data are secure from potential threats and vulnerabilities. To achieve this, CIOs should implement robust cybersecurity measures such as firewalls, intrusion detection systems, and encryption technologies to protect against unauthorized access and data breaches. They should also implement access controls to ensure that only authorized personnel have access to sensitive data and systems. Furthermore, CIOs should prioritize cybersecurity awareness and training for employees, regularly conduct security audits and vulnerability assessments, and comply with relevant regulations and standards to maintain the highest level of cybersecurity.
By taking these steps, CIOs can help protect their organization's sensitive data, intellectual property, and reputation from the growing threat of cyber attacks.

**PANELISTS**



**Sajed Naseem**
CISO
New Jersey Judiciary

## Closing Remarks & Raffle Giveaway

5:20 PM-5:30 PM

## Cocktail Reception

5:30 PM-6:30 PM

IN PARTNERSHIP WITH

chronosphere KnowBe4 Human error. Conquered. RegScale Synack SauceLabs Reco CYERA