

# AGENDA

## The Future of Cybersecurity CISO Think Tank

### SPEAKERS



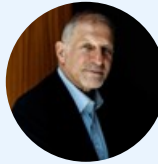
**Leo Cunningham**  
CISO  
[Owkin Inc](#)



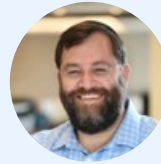
**Ania Kowalczyk**  
VP of Information  
Security Risk and  
Compliance  
[MongoDB](#)



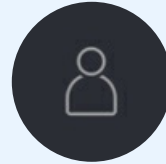
**Melissa Ouari**  
InfoSec Risk &  
Business Continuity  
Officer  
[Money Management  
International](#)



**Henry Weingarten**  
Managing Director  
and CIO  
[The Astrologers Fund](#)



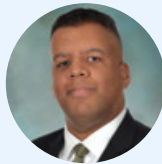
**Israel Bryski**  
Head of Information  
Security  
[MIO Partners](#)



**Sara Aby**  
CTO



**Harry Halikias**  
Sr. Director, Global  
Information Security  
[Sony Music  
Publishing](#)



**Todd Gordon**  
Security Director  
[Eisner Advisory  
Group](#)



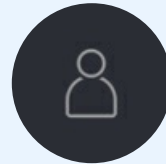
**Yabing Wang**  
CISO  
[Justworks](#)



**Matthew Martin**  
Founder  
[Two Candlesticks](#)



**Mark Jankiewicz**  
Commercial Chief  
Risk Officer  
[Conduent](#)



**Arvin Bansal**  
CISO



**Edmond Mack**  
CISO  
[Cencora](#)



**Alex Shulman**  
Managing Director,  
Cloud Security  
[Ernst & Young](#)



**Jim Rutt**  
CIO/CISO  
[The Dana  
Foundation](#)



**Amit Basu**  
VP, CIO & CISO  
[International  
Seaways](#)



**Chris Hickman**  
Chief Security Officer  
[Keyfactor](#)



**Cedric Curry**  
CISO  
[NYC Citywide  
Administrative  
Services](#)



**Sateesh Challa  
Kumar**  
Head of Digital  
Transformation  
Office  
[Societe Generale](#)



**Rahul Bhardwaj**  
CISO - Cyber and  
Data Privacy | Head  
Information Security  
[EXL](#)



**Anthony Gonzalez**  
Principal, Strategic  
Advisor  
[Innervation Services  
LLC](#)



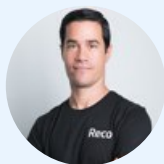
**Matt Goldberg**  
Chief of Staff (Office  
of the CISO)  
[Clear](#)



**Melody Balcet**  
CEO, WGI  
Corporation / Former  
Head of Digital,  
Resilience.  
[Barclays](#)



**Danny Brickman**  
Co-Founder & CEO  
[Oasis Security](#)



**Ofer Klein**  
Co-Founder & CEO  
[Reco](#)



**Jacob Thampi**  
VP, Divisional  
Information Security  
Officer  
[QBE North America](#)



**Samrah Kazmi**  
Chief Innovation  
Officer  
[RESRG](#)

[Click Here to Register](#)



**February 22, 2024**

Eastern Time

**Registration**

**8:30 AM-9:00 AM**

**Morning Networking**

**9:00 AM-9:30 AM**

**Opening Remarks**

**9:35 AM-9:45 AM**

**VISION VOICES KEYNOTE**

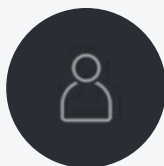
**Securing Growth: Cybersecurity Considerations in  
Mergers and Acquisitions**

**9:45 AM-10:10 AM**

[www.cvisionintl.com](http://www.cvisionintl.com)

Dive into the critical intersection of cybersecurity and M&A activities, where the stakes are high and the risks are significant. Arvin Bansal explores the unique challenges and complexities of integrating cybersecurity strategies during mergers, acquisitions, and divestitures. Gain insights into effective risk assessment methodologies, due diligence practices, and post-transaction integration strategies to safeguard sensitive data and mitigate potential threats. Join Arvin as he navigates the evolving landscape of cybersecurity in M&A transactions and explores best practices for ensuring security and compliance throughout the deal lifecycle.

#### PANELISTS



Arvin Bansal  
CISO

#### FIRESIDE CHAT

10:15 AM-10:50 AM

### Navigating AI Security in the Cloud: CISO Insights for 2024

"Navigating the Cloud" panel will focus on CISOs and InfoSec leaders exploring how to secure AI data in the evolving cloud landscape. Focused on AI security best practices, encryption, and threat intelligence, the session offers actionable insights from real-world experiences. The discussion extends to specialized topics like Zero Trust Architecture, regulatory compliance, AI-centric incident response, and vendor risk management. Engage with industry leaders for collaborative discussions, empowering CISOs with practical strategies to navigate the complexities of AI security in the cloud. Don't miss this session for essential insights into securing AI data in the dynamic cloud environment of 2024.

#### CHAIR



Rahul Bhardwaj  
CISO - Cyber and  
Data Privacy | Head  
Information Security  
EXL

#### PANELISTS



Alex Shulman  
Managing Director,  
Cloud Security  
Ernst & Young



Harry Halikias  
Sr. Director, Global  
Information Security  
Sony Music  
Publishing

#### Coffee Break

10:50 AM-11:15 AM

#### VISION VOICES

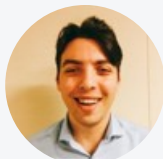
11:15 AM-11:30 AM

### Enterprise Risk and Probability Theory

In today's complicated cyber environment, the significance of a risk-centric approach is paramount. Explore the importance of adopting a risk mindset as a core in building your security strategy and ensuring buy-in from senior leaders.

Cyber Security is fundamentally a risk management function. We must know and understand our risks to effectively drive prioritization, but your picture is only as strong as your assumptions. There's no magic crystal ball, but you can increase the confidence in your risk picture and generate buy-in from stakeholders using simple probability models. Join me as I outline these methods and show what you need to get started.

#### PANELISTS



**Matt Goldberg**  
Chief of Staff (Office  
of the CISO)  
[Clear](#)

#### DISRUPTOR

11:35 AM-11:50 AM

### Navigating Post-Quantum Cryptography: Communicating Cyber Risk at Board-Level

Ready or not, a new era for security is on the not-so-distant horizon, and there's no shortage of hype surrounding quantum computing. But the most critical question security and business leaders must ask now is how will post-quantum cryptography (PQC) impact cybersecurity?

In this session, Chris Hickman, Chief Security Officer at Keyfactor, will share his expert views on the impact of quantum computing and what it will take to become quantum-ready – from the art of strategic planning and decision-making to communicating the potential cyber risk at the board level.

Post-quantum cryptography will affect everything we do, and adapting accordingly is inevitable. Whether you're a CISO worried about Q-Day timing or complying with new industry standards around PKI and code signing, you won't want to miss this!

#### PANELISTS



**Chris Hickman**  
Chief Security Officer  
[Keyfactor](#)

### Lunch & Disruptor Showcase

12:00 PM-1:00 PM

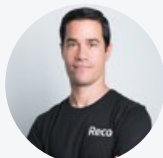
#### DISRUPTOR

12:40 PM-12:55 PM

### Leveraging Artificial Intelligence for SaaS Discovery

In today's interconnected business world, companies rely on SaaS applications as the operating system of business, which can pose significant cybersecurity risks. This makes it critical for companies to have effective security measures in place to properly secure their entire SaaS environment. Failure to do so can result in data breaches, financial losses, and reputational damage. To mitigate this risk, companies must ensure they are monitoring not only the SaaS applications that are managed and known to the IT team, but their entire SaaS environment. Application discovery provides a comprehensive view into the entire SaaS ecosystem, including what managed applications have access to data, connected third-party apps, and even shadow apps, as well as who has enabled them, and the level of access they've been granted. Using a combination of graph algorithms, anomaly detection, NLP, and GenAI tools, solutions leveraging AI can provide a complete picture of interactions and activities across users. This insight can be used to pinpoint common causes of a breach such as misconfigurations, overly permissioned users, and compromised accounts. In this session, we'll explore the importance of investing in SaaS discovery, how AI can add the context needed to protect against common causes of breaches, and how organizations can secure their SaaS from the most common risks that can lead to a breach in 2023 and beyond.

#### PANELISTS



**Ofer Klein**  
Co-Founder & CEO  
[Reco](#)

#### KEYNOTE PANEL

1:00 PM-1:55 PM

### Building Cyber Fortitude: Digital and Risk Strategies for Resilient Cybersecurity

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 and digital 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.

#### CHAIR



**Leo Cunningham**  
CISO  
[Owkin Inc](#)

#### PANELISTS



**Sateesh Challa Kumar**  
Head of Digital Transformation Office  
[Societe Generale](#)



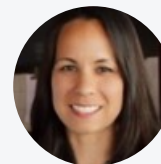
**Jacob Thampi**  
VP, Divisional Information Security Officer  
[QBE North America](#)



**Cedric Curry**  
CISO  
[NYC Citywide Administrative Services](#)



**Samrah Kazmi**  
Chief Innovation Officer  
[RESRG](#)



**Melody Balcet**  
CEO, WGI Corporation / Former Head of Digital Resilience  
[Barclays](#)

### Networking Break

2:00 PM-2:20 PM

## PANEL

2:20 PM-3:05 PM

# Ransomware and Cyber Readiness

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



**Jim Rutt**  
CIO/CISO  
The Dana  
Foundation

### PANELISTS



**Melissa Ouari**  
InfoSec Risk &  
Business Continuity  
Officer  
Money Management  
International



**Edmond Mack**  
CISO  
Cencora



**Amit Basu**  
VP, CIO & CISO  
International  
Seaways

## DISRUPTOR

3:10 PM-3:25 PM

# Safeguarding Non-Human Identities: Insights from Recent Breaches

Recent security breaches, exemplified by incidents such as Cloudflare's, serve as a poignant reminder of the vulnerabilities inherent in unattended Non-Human Identities (NHIs). These breaches underscore the intricate operational hurdles even the most seasoned security teams encounter in managing NHIs effectively. While modern enterprises have diligently crafted strategies to fortify human identities and have deployed tailored solutions accordingly, the same rigor is often lacking in the realm of NHIs. In this exclusive session, esteemed Oasis Security CEO, Danny Brickman, will expound upon how organizations can significantly curtail their susceptibility to breaches by implementing robust NHI management practices, thereby diminishing their attack surface and fortifying their cyber defenses.

### PANELISTS



**Danny Brickman**  
Co-Founder & CEO  
Oasis Security

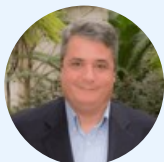
## FIRESIDE CHAT

3:30 PM-4:05 PM

## Third-Party Exposure

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



**Jim Rutt**  
CIO/CISO  
The Dana  
Foundation

### PANELISTS



**Mark Jankiewicz**  
Commercial Chief  
Risk Officer  
Conduent



**Yabing Wang**  
CISO  
Justworks

## Closing Remarks & Raffle Giveaway

4:05 PM-4:15 PM

## Cocktail Hour

4:15 PM-5:15 PM

IN PARTNERSHIP WITH



**TWO  
CANDLESTICKS**

**KEYFACTOR**

**THREATLOCKER®**

ZERO TRUST ENDPOINT SECURITY

**reco**



**SEAL SECURITY**



**ZAFRAAN**

**OASIS**