

# AGENDA

## The Future of Cybersecurity CISO Think Tank

### SPEAKERS



**Max Gill**  
Global Head of Cyber  
Security  
[BionicalEmas](#)



**Jenna Franklin**  
Partner  
[Stephenson  
Harwood](#)



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



**Rami El Outa**  
Regional IT Director -  
Infrastructure,  
Solutions and  
Cybersecurity  
[Grupo Eurofins](#)



**Lida Rragami**  
Heah of Cyber  
Security  
[Sonnedix](#)



**Simon Mair**  
CISO  
[National Bank of  
Kuwait International](#)



**Eri Kejser**  
Director of Security &  
Cloud  
Transformation  
[FORCE Technology](#)



**Mike Backinsell**  
Global Deputy CISO  
[ManpowerGroup](#)



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



**Andrew Fleming**  
MI and Reporting  
EMEA Head  
[Deutsche Bank](#)



**Khadir Fayaz**  
SVP Digital &  
Technology  
[CBRE](#)



**Robin Smith**  
CISO  
[Aston Martin](#)



**Himanshu Jha**  
Former Cloud CTIO  
[TSB Bank](#)



**Cornelius Namiluko**  
Managing Director -  
Global Co-Head of  
Security Architecture  
[Goldman Sachs](#)



**Ky Nichol**  
CEO  
[Cutover.](#)



**Fox Ahmed**  
Global Head of  
Cybersecurity &  
Technology and Data  
Protection  
Regulatory Risk  
[BNP Paribas](#)



**Aman Thind**  
CTO  
[State Street](#)



**Azeem Aleem**  
Managing Director  
(MD) Client  
Leadership, EMEA  
[Sygnia](#)



**Adam Denyer-Hampton**  
Director of Solutions  
Architects,  
International  
Markets  
[SecurityScorecard](#)



**Pam Balsam**  
Snr. Regional  
Enterprise Account  
Manager  
(International)  
[KnowBe4](#)



**Andrew Bagguley**  
CISO  
[Liiv](#)

[Click Here to Register](#)



**February 27, 2024**

United Kingdom 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

### **Darwin & the Accelerationist Machines: AI's Future Paths**

9:40 AM-10:05 AM

Embark on an exploration in "Darwin & the Accelerationist Machines," where we unravel the past and future of Artificial Intelligence (AI) and its transformative role in society. The session delves into the synergy of AI and human consciousness, reviewing George Dyson's insights on the emergence of a conscious mind from today's technology and how it shapes the future of technologies. With a focus on the radical school of Accelerationism, the discussion navigates the far-reaching societal impact of AI, addressing ethical considerations and emphasizing the role of Cybernetics in harnessing its power.

## PANELISTS



**Robin Smith**  
CISO  
Aston Martin

## KEYNOTE

10:10 AM-10:35 AM

### Tactics Tool and Procedures? Where the rubber meets the road: Learning from a Heavyweight Attack

In recent years, the Sygnia Incident Response Team has handled numerous nation-state attacks that employed unique attack techniques and posed new challenges to security leaders and incident responders.

In this talk we will guide you through the anatomy of a real-world attack we recently responded to, including attacker TTPs and effective response procedures. This case study will highlight the common pitfalls and key opportunities when defending against even the most sophisticated attacks.

## PANELISTS



**Azeem Aleem**  
Managing Director  
(MD) Client  
Leadership, EMEA  
Sygnia

## Coffee Break

10:35 AM-11:10 AM

## VISION VOICES KEYNOTE

11:10 AM-11:35 AM

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

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



**Aman Thind**  
CTO  
State Street

## PANEL

11:40 AM-12:25 PM

# Ransomware and Cyber Readiness

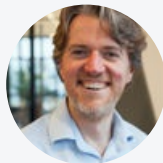
Ransomware attacks are becoming increasingly prevalent and sophisticated, affecting businesses and individuals in all sectors. In 2024, these attacks are expected to continue to grow, resulting in significant financial losses, data theft, and reputational damage. Businesses should implement comprehensive security measures, including regular backups, employee training, and endpoint security, to minimize the risk of a ransomware attack. Additionally, because cyber attacks are unpredictable and complex it's important to have cyber recovery plans in place to orchestrate both teams and technology to minimize the impact of an attack. Businesses must develop recovery plans detailing the tasks to restore systems, manage data integrity, keep stakeholders informed of progress and meet regulatory requirements.

## CHAIR



**Leo Cunningham**  
CISO  
Owkin Inc

## PANELISTS



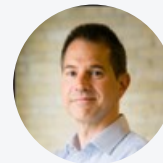
**Ky Nichol**  
CEO  
Cutover.



**Simon Mair**  
CISO  
National Bank of  
Kuwait International



**Fox Ahmed**  
Global Head of  
Cybersecurity &  
Technology and Data  
Protection  
Regulatory Risk  
BNP Paribas



**Mike Backinsell**  
Global Deputy CISO  
ManpowerGroup

## Lunch & Vision Voice

12:25 PM-1:25 PM

## VISION VOICES

1:25 PM-1:40 PM

# What is Wrong With Security and How to Fix It

Computer systems are complex. Complexity makes it difficult to understand what is going and thus how to secure a system. To deal with complexity, the theory of abstraction is a powerful approach that allows us not only to simplify how to reason about a system, but also forces us to hide unnecessary details. I argue that this is where security starts to go wrong. Abstractions are a double-edged; on one hand helping us to deal with complexity and on another hides crucial information (such as interfaces or vulnerabilities in an underlying system) needed to secure the system. Attackers are constantly exploiting assumptions made in the various layers of abstractions. This is what is wrong with security. To fix this, we should have assumptions, security properties and responsibilities model explicitly defined at every layer of abstraction and tooling to enable validation of these. Developers relying on an underlying system would use that to build

their own assumptions while ensuring that the assumptions of underlying components are validated.

#### PANELISTS



**Cornelius Namiluko**  
Managing Director -  
Global Co-Head of  
Security Architecture  
[Goldman Sachs](#)

#### VISION VOICES

1:45 PM-2:15 PM

## Navigating the Interplay between UK and International Data AI Regulation in the Digital Age

This session explores the intricate relationship of the UK and International regulatory compliance in data protection, privacy concerns, artificial intelligence (AI), and ethical considerations in the contemporary digital landscape. It delves into how organizations and their partners must adhere to UK and International regulations while leveraging AI-driven data insights and upholding ethical standards and individual privacy rights. The discussion will encompass the challenges, strategies, and emerging trends in this complex domain within the context of the UK and the International regulatory landscape.

#### PANELISTS



**Jenna Franklin**  
Partner  
[Stephenson](#)  
[Harwood](#)

#### DISRUPTOR

2:20 PM-2:35 PM

## Enhancing the Resilience of Your Organization's Final Barrier: The Human Firewall

In today's digital landscape, social engineering attacks like phishing, Business Email Compromise (BEC), and Ransomware are increasingly prevalent. These cunning tactics rely on manipulating humans to gain unauthorized access to protected systems and sensitive data. As the frequency of such cyber-attacks rises, it is crucial to fortify your organization's last line of defense: the human firewall.

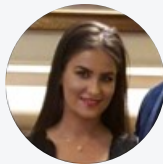
In this session we will look into case studies around:

Regular, tailored security awareness training to educate employees about social engineering threats.

Foster a reporting culture for prompt identification of suspicious activities.

Strengthen password policies and use multi-factor authentication (MFA) to reduce risks.

## PANELISTS



**Pam Balsam**  
Snr. Regional  
Enterprise Account  
Manager  
(International)  
[KnowBe4](#)

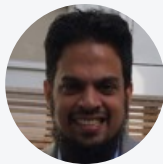
## VISION VOICES

2:40 PM-2:55 PM

### The Rise of AI: Cyber Innovation & Risk Impact

AI is creating massive transformation impacts across businesses, from healthcare to financial services. The rise of GenAI and advanced AI capabilities poses a significant opportunity to advance organizational cyber maturity. These include automation in vulnerability remediation to predictive threat insights. On the contrary, the acceleration of AI services also poses a significant risk to businesses. In this session, we will explore pragmatic approaches to leveraging AI for cyber innovation while ensuring sufficient guardrails are developed to enable business acceleration using secure AI services.

## PANELISTS



**Khadir Fayaz**  
SVP Digital &  
Technology  
[CBRE](#)

## Networking Break

2:55 PM-3:10 PM

## PANEL

3:10 PM-3:55 PM

### Scaling your Third Party Risk Program in the World of Automated Attacks

One of the largest obstacles facing companies today is to “do more with less” in the world of automated attackers. Increasingly we are being asked to reduce risk, increase the scope of coverage and continually protect our organisations from emerging threats. With the introduction of highly targeted automated attacks across multiple industries and countries. As well as governing bodies such as the EU introducing legislation and compliance requirements, which offer severe penalties to those organisations that are not implementing sufficient third party risk programs. This session will discuss how organisations across all industry verticals are implementing automated workflows and using global data sets to protect their organisations from the third party breaches and incidents.

#### CHAIR



**Leo Cunningham**  
CISO  
Owkin Inc

#### PANELISTS



**Lida Rragami**  
Head of Cyber  
Security  
Sonnedix



**Andrew Fleming**  
MI and Reporting  
EMEA Head  
Deutsche Bank



**Adam Denyer-Hampton**  
Director of Solutions  
Architects,  
International  
Markets  
SecurityScorecard

#### VISION VOICES

4:00 PM-4:15 PM

### A CISO Needs to Meet Their Board's Expectations, Communicate Effectively with Them, and Earn Their Trust. What's the Best Approach?

The CISO plays a critical role in communicating with the board of an organisation, ensuring that cybersecurity concerns are effectively conveyed and understood. This communication involves presenting comprehensive risk assessments, threat landscapes, and the effectiveness of current security measures. The CISO must articulate complex technical concepts in a business-friendly language, emphasising the potential impact of cyber threats on the organisation's overall strategy and objectives. Additionally, regular updates on cybersecurity initiatives, compliance status, and incident response plans are crucial to maintaining the board's confidence. Successful CISO-board communication enhances the organisation's cyber resilience, aligning security efforts with broader business goals.

#### PANELISTS



**Eri Kejser**  
Director of Security &  
Cloud  
Transformation  
FORCE Technology

#### Networking Break

4:15 PM-4:30 PM

#### VISION VOICES

4:30 PM-4:45 PM

### Creating and Delivering a Security Upgrade Program

Following a significant ransomware attack, a leading biotech giant reevaluated its cybersecurity approach. Rami will discuss the tactical and strategic measures taken post-incident, emphasizing the roadmap for implementation. The focus is on elevating cybersecurity maturity through advanced technologies, fortified defenses, and a holistic strategy. Rami will delve into integrating cybersecurity into the broader business approach, fostering awareness, and collaborative efforts across departments. The session aims to provide insights and

guidance for organizations seeking to enhance their cybersecurity resilience in the face of evolving digital threats.

#### PANELISTS



**Ramí El Outa**  
Regional IT Director -  
Infrastructure,  
Solutions and  
Cybersecurity  
[Grupo Eurofins](#)

#### VISION VOICES

### Guarding the Cloud: Navigating the Rising Tide of Cloud Vulnerabilities and Cyber Threats in 2024

4:50 PM-5:05 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 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.

#### PANELISTS



**Himanshu Jha**  
Former Cloud CTIO  
[TSB Bank](#)

### Closing Remarks & Raffle Giveaway

5:05 PM-5:10 PM

### Cocktail Hour

5:10 PM-6:10 PM

IN PARTNERSHIP WITH





**TWO  
CANDLESTICKS**

SYGNIA

**cutover**

**KnowBe4**  
Human error. Conquered.

**reco**

**THREATLOCKER®**

ZERO TRUST ENDPOINT SECURITY