

# AGENDA

## The Future of Cybersecurity CISO Think Tank

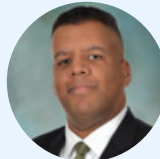
### SPEAKERS



**Anthony Gonzalez**  
Former VP & CISO  
[QBE North America](#)



**Jordan Tannenbaum**  
MD  
CIO/CMIO  
[Saint Peter's Healthcare System](#)



**Todd Gordon**  
CISO  
[EisnerAmper](#)



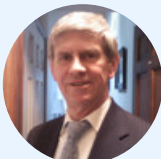
**Ariel Weintraub**  
CISO  
[MassMutual](#)



**Cindy Cullen**  
Global Director of  
Information Security  
[NDegrees](#)



**Johnny Wong**  
Senior Director,  
Solutions  
Architecture  
[Veracode](#)



**Ivan Durbak**  
CIO  
[Bronx Lebanon Hospital Center](#)



**Adam Healy**  
CSO  
[BlockFi](#)



**Chris Strand**  
Chief Risk and  
Compliance Officer  
[Cybersixgill](#)



**Michael Gross**  
Manager,  
Cybersecurity  
Intelligence  
[Cleveland Clinic](#)



**Tim Swope**  
CISO  
[Catholic Health System](#)



**Chris Williamson**  
SVP Information  
Systems and Security  
[Myriad Genetics](#)



**Ganesh Pai**  
Founder & CEO  
[Uptycs](#)



**Martin Howard**  
EVP/IT & IS  
[Fortium Partners](#)



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



**Lena Smart**  
CISO  
[MongoDB](#)



**David Cass**  
CISO  
[Law and Forensics](#)



**Johnny Wong**  
Senior Director,  
Solutions  
Architecture  
[Veracode](#)



**John Whiting**  
Global CSO  
Omnicom



**Anthony Gonzalez**  
CISO NA  
QBE North America



**David Cass**  
CISO  
GSR



**Martin Howard**  
EVP/CIO  
Avesis



[Click Here to Register](#)



**February 23, 2022**

Eastern Time

## Welcome & Registration

12:00 PM-12:30 PM

### KEYNOTE PANEL

## Keynote Panel: Security Controls: Measuring Efficacy for the Business Growth

12:30 PM-1:25 PM

The industry is spending record amounts on cybersecurity tooling, but somehow CISOs still are at times left scrambling to respond to the vulnerabilities like Log4j. Assuming that these types of critical and far-reaching events are inevitable, how can CISOs further improve their organization's preparedness for future cyberattacks?

This panel will discuss potential strategies for determining the critical security controls - both technology and behavioral - that can minimize cyber-risks and give the organization the competitive advantage to grow and innovate. We will explore frameworks for measuring the efficacy of cybersecurity investments, and KPIs that show the board the investment is safeguarding the company's digital infrastructure for the long term.

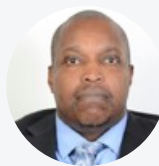
## PANELISTS



**Chris Williamson**  
SVP Information  
Systems and Security  
Myriad Genetics



**Ganesh Pai**  
Founder & CEO  
Uptycs



**John Whiting**  
Global CSO  
Omnicom



**Anthony Gonzalez**  
CISO NA  
QBE North America

## Fireside Chat: Technology Supply Chain

1:30 PM-2:15 PM

Many large enterprises in today's fiercely competitive climate look toward optimizing its supply chain to increase business scale and agility. By harnessing a combination of technologies like artificial intelligence, machine learning, and predictive analytics, companies can automate and create new customer experiences that increase satisfaction and boost sales. Gaps remain in supply chain cyber security even as digitalization accelerates. By doing so, companies are left vulnerable to the growing risk of a cyber-attack. There are no shortage of stories illustrating the dangers of lax cyber security, with the biggest attacks able to utterly paralyze an operation and cause millions in losses. Despite this obvious danger, efforts to improve cyber security are progressing slowly. Future risks to the supply chain will involve software, cloud-based infrastructures, and hyper-converged products, rather than simply hardware. Even after many years of experience, capable CISOs find they may not be equipped to overcome the cybersecurity concerns that arise from building control contractors.

### CHAIR



**Chris Strand**  
Chief Risk and  
Compliance Officer  
Cybersixgill

### PANELISTS



**Ariel Weintraub**  
CISO  
MassMutual



**Adam Healy**  
CSO  
BlockFi

## Networking Break

2:15 PM-2:30 PM

## Keynote Panel: Being Effective.... Securely

2:30 PM-3:25 PM

In the post pandemic era, remote employment is the new status quo. Employers are forced to implement and improve the digital workplace by providing productivity tools and accessibility to company resources. In this session, we will share case studies of successful

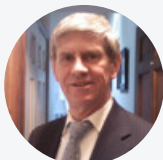
digital workplace implementations, including how to deal with the inherent security risks of expanded accessibility to company resources. In this session you will learn from real working examples the keys to implementing a successful digital workplace including how to evaluate the potential ROI from the different security strategies available.

#### CHAIR



**David Cass**  
CISO  
Law and Forensics

#### PANELISTS



**Ivan Durbak**  
CIO  
Bronx Lebanon  
Hospital Center



**Martin Howard**  
EVP/IT & IS  
Fortium Partners



**Cindy Cullen**  
Global Director of  
Information Security  
NDegrees



**Lena Smart**  
CISO  
MongoDB

## Networking Break

3:25 PM-3:40 PM

## Disruptor: Guarding the Doors: Navigating Risk From Third-Party Code

3:40 PM-4:05 PM

Open source libraries are widely leveraged by developers. In fact, 97 percent of the typical Java application is made up of open source libraries. But nearly 80 percent of developers never update third-party libraries after including them in codebase.

What does this mean for your applications? There is a good chance that your third-party libraries have undetected vulnerabilities. Scary, right?

The good news is that when alerted to vulnerabilities in open source libraries, developers tend to act quickly. This is especially true when developers understand how the vulnerability could impact their application.

Join us as we review our annual study on open source libraries, State of Software Security (SOSS) v12: Open Source Edition. We will explore the most popular open source libraries, how libraries are evaluated and selected, and how to eliminate risk by fixing vulnerabilities.

#### PANELISTS



**Johnny Wong**  
Senior Director,  
Solutions  
Architecture  
Veracode

## Panel: Human Security Engineering

4:10 PM-5:05 PM

90%+ of all losses result from attacks targeting users, honest users. A common solution to user error is awareness, but we need to fix the system that facilitated the creation of the error, the action, and the results, which means not just stopping errors but also accidents and malice. In this session we will share a model of Human Security Engineering identifying the optimal suite of countermeasures, and work

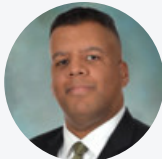
through user targeting attacks to experience implementing the model. This talk will also look at a comprehensive strategy to address the insider threat, whether it results from malicious or well-meaning insiders, while detailing HSE and providing the resources required for attendees to follow up and consider how they can implement HSE to better mitigate their own insider threats.

#### CHAIR

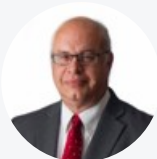


**David Cass**  
CISO  
Law and Forensics

#### PANELISTS



**Todd Gordon**  
CISO  
EisnerAmper



**Jordan Tannenbaum**  
MD  
CIO/CMIO  
Saint Peter's  
Healthcare System



**Tim Swope**  
CISO  
Catholic Health  
System



**Michael Gross**  
Manager,  
Cybersecurity  
Intelligence  
Cleveland Clinic



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

## Raffle & Closing Remarks

5:05 PM-5:15 PM

## Cocktail Hour

5:15 PM-6:30 PM

IN PARTNERSHIP WITH

