

# AGENDA

## The Future of Cybersecurity CISO Think Tank

### SPEAKERS



**Christopher Reed**  
Cyber Security  
Engagement  
Manager  
*Tata Consultancy  
Services*



**Kristen Chapman**  
Senior Director,  
Privacy Technology  
*Salesforce*



**Sue Bergamo**  
CISO  
*BTE Partners*



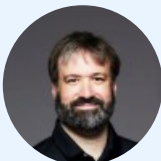
**Grace Beason**  
Director of GRC  
*Guidewire Software*



**Michael Woodson**  
Director of  
Information Security  
*Sonesta  
International Hotels  
Corporation*



**Wes Kussmaul**  
CIO  
*Authenticity Institute*



**David Matousek**  
Director of  
Cybersecurity  
*John Hancock*



**Brian Lowy**  
Director, IS  
*Investnet*



**Radha Kuchibhotla**  
VP, IT  
*Accenture*



**Iorraine spadaro**  
CIO  
*Global Partners LP*



**Jim Haynie**  
Director, Information  
Technology  
*Oasis Systems*



**Derek Donahue**  
Regional Sales  
Director, North  
East/Eastern Canada  
*Forward Networks*



**Robert Clougherty**  
Ph.D.  
CIO  
*Drew University*



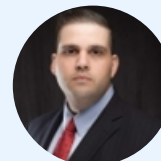
**Sanjay Srivastava**  
Global CDO  
*Genpact*



**Shishir Shekhar**  
Sr. Director & Global  
Lead - Innovation  
and Technology  
Strategy  
*Landis+Gyr*



**DAN BENJAMIN**  
CEO & CO-FOUNDER  
*Dig Security*



**Kevin Papadopoulos**  
Principal, Director of  
Investment  
Technology & CISO  
*Longfellow  
Investment  
Management Co*



**Chris Eng**  
Chief Research  
Officer  
*Veracode, Inc.*



**Tomas Persson**  
CISO  
Omegapoint

[Click Here to Register](#)



**June 08, 2023**

Eastern Time

## Registration

9:30 AM-10:15 AM

## Morning Networking

10:15 AM-11:00 AM

## Opening Remarks

11:00 AM-11:05 AM

### KEYNOTE

## Generative AI and Digital Transformation: Unleashing Innovation and Shaping the Future

11:10 AM-11:35 AM

This Keynote explores the intersection of generative AI and digital transformation, highlighting the practical use case applications for businesses and the role of CIOs in leveraging their potential. Generative AI empowers organizations to enhance creativity, engage customers, overcome data limitations, optimize autonomous systems, and improve communication through automated content creation and language services. As part of the broader digital transformation journey, CIOs recognize generative AI as a transformative tool that drives innovation, fosters agility, and shapes the future of their organizations. By embracing generative AI as a strategic component of digital transformation, businesses can unlock new possibilities and gain a competitive edge in the rapidly evolving technological landscape.

### PANELISTS



**Sanjay Srivastava**  
Global CDO  
Genpact

### PANEL

11:40 AM-12:25 PM

# The Promising 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.

## CHAIR



**Sue Bergamo**  
CISO  
BTE Partners

## PANELISTS



**Michael Woodson**  
Director of  
Information Security  
Sonesta  
International Hotels  
Corporation



**Robert Clougherty**  
Ph.D.  
CIO  
Drew University



**Chris Eng**  
Chief Research  
Officer  
Veracode, Inc.



**Tomas Persson**  
CISO  
Omegapoint

## Networking Lunch

12:25 PM-1:30 PM

## DISRUPTOR

### Tackling Data Security in the Multi-Cloud Era

1:30 PM-1:45 PM

This year, the amount of data in public clouds has surpassed that residing on-prem. As such, enterprises no longer maintain full visibility, control, and governance of their data – for which they pay a steep price.

In this session, Dan Benjamin, Co-Founder and CEO of Dig Security, will explain how organizations must approach data security in the multi-cloud era.

With the cost of data breaches reaching all-time highs, protecting customer information has become the number one challenge for modern organizations.

Dan will highlight the key capabilities organizations should look for in a cloud data security solution, including data security posture management (DSPM), real-time data detection and response (DDR), and cloud data loss prevention (cloud DLP).

He will also dive deeper into three areas impacted by the mass migration of data to the cloud: privacy

to address regulatory compliance capabilities; governance

to determine who's entitled to data access and sharing privileges and to define data ownership, accountability, and collaboration; and security

to protect locations where sensitive data typically resides.

## PANELISTS



**DAN BENJAMIN**  
CEO & CO-FOUNDER  
Dig Security

## VISION KEYNOTE PANEL

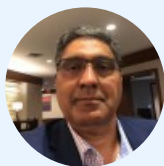
1:50 PM-2:35 PM

### Bridging the Gap Between IT and the Business

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

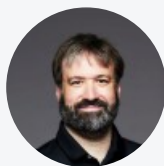


**Radha Kuchibhotla**  
VP, IT  
[Accenture](#)

#### PANELISTS



**Iorraine Spadaro**  
CIO  
[Global Partners LP](#)



**David Matousek**  
Director of  
Cybersecurity  
[John Hancock](#)



**Kevin Papadopoulos**  
Principal, Director of  
Investment  
Technology & CISO  
[Longfellow  
Investment  
Management Co](#)



**Shishir Shekhar**  
Sr. Director & Global  
Lead - Innovation  
and Technology  
Strategy  
[Landis+Gyr](#)

## Networking Break

2:35 PM-3:00 PM

## DISRUPTOR

3:00 PM-3:15 PM

### How to Ensure a Reliable, Predictable, and Secure Network With a Digital Twin

A network digital twin, based on a mathematical model, is a necessary tool to modernize mission-critical networks and to reduce cybersecurity risk.

It provides vendor-agnostic insight into network behavior, offers detailed visualization and verifies that the network is behaving according to the operator's intent. Functionality like search, modeling, and intent checks help engineering teams reduce MTTR, avoid outages, verify security posture, and ensure policy compliance across all network environments -- on-prem, cloud, and multi-cloud.

Derek Donahue will discuss how Fortune 500 businesses use a digital twin to make their network reliable, agile, and secure.

#### PANELISTS



**Derek Donahue**  
Regional Sales  
Director, North  
East/Eastern Canada  
[Forward Networks](#)

## PANEL

3:20 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 2023, 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 2023 and beyond.

#### CHAIR



**Sue Bergamo**  
CISO  
BTE Partners

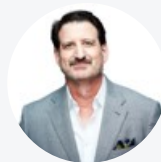
#### PANELISTS



**Wes Kussmaul**  
CIO  
Authenticity Institute



**Grace Beason**  
Director of GRC  
Guidewire Software



**Brian Lowy**  
Director, IS  
Investnet



**Jim Haynie**  
Director, Information  
Technology  
Oasis Systems

## Closing Remarks & Raffle Giveaway

4:05 PM-4:10 PM

## Cocktail Hour

4:10 PM-5:10 PM

TOGETHER WITH

