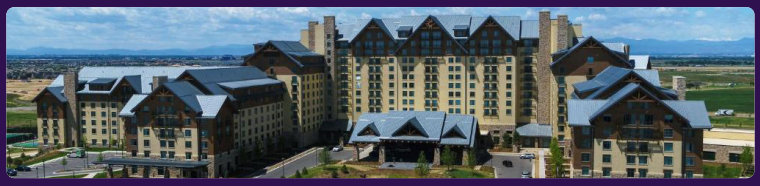
AGENDA

NORTH AMERICAN INFORMATION SECURITY SUMMIT
NAISS24
June 16-18, 2024 | Denver, CO



Gaylord Rockies Resort & Convention Center

JUNE 16, 2024

5:00 pm - 6:10 pm

Panel Discussion: Women in Security

- Creating a purpose-driven strategy that makes an impact as our organization grows and nurtures a diverse workforce
- Understanding the leader's role as a force to shape and demonstrate corporate culture, and to serve as a catalyst for equality and inclusion
- Sharing typical challenges faced by corporations when trying to promote diversity in the workforce
- Illustrating the importance of today's leaders building up and supporting the next generation our organizations will need for the future. What does that look like on a day-to-day basis?
- Offering examples of strong and effective mentorship programs in onboarding, cross-training, job shadowing, and continuing education that make the difference

Stacee Jones
Deputy Chief Information Security Officer & IT Director
Lear Corporation

Linda Marcone
CISO
Crate & Barrel

Jennifer Franks
Director, Center for Enhanced Cybersecurity
US Government Accountability Office

Lawana Jones
SVP, Chief Technology Officer
United Way Worldwide

Hazleena Hashim
Chief Information Officer
Natural Habitat Adventures

6:15 pm - 7:30 pm

WELCOME Drinks RECEPTION

AGENDA

JUNE 17, 2024

7:30 am - 8:15 am — **Registration & Breakfast**

8:15 am - 8:20 am — **Opening Remarks and Important Announcements**

8:20 am - 8:30 am — **Chair's Welcome Address**

Tomás Maldonado
Chief Information Security Officer
National Football League

8:30 am - 9:05 am — **The People-Led, Tech-Powered Future of Cybersecurity**

- Evolution of CISO (from back office to front office as business leaders)
- Importance of digital trust (e.g., how to earn it, how to keep it, how to grow it)
- Challenges and opportunities with regulation and consolidation
- Tech-enabled, human-in-the-loop approach to managing regulation, consolidation and customer trust

Jason ODell
VP, Security Operations
Walmart

9:05 am - 9:40 am — **A CISO's Guide to the AI Threatscape**

- Why should CISOs care about not only responding to cyber events, but also recovering from them?
- How we are seeing attackers adopt and deploy AI now and ways to get ahead of future risk
- Balancing the good and bad of Generative AI in your businesses: Efficiency VS risk
- How CISOs should prepare moving forward and ensure your teams are ready through upskilling and adequate education
- Key strategies for building an ideal cyber resilience framework

Xochitl Monteon
VP Cybersecurity & Chief Privacy Officer
Intel

AGENDA

ROOM 1 CHAIR

Tomás Maldonado
Chief Information Security Officer
National Football League

ROOM 2 CHAIR

TBA

9:45 am - 10:20 am

WORKSHOP
BREAKOUT ROOM 1

Navigating the Challenges of Security in Serverless

- Does spending less time thinking about infrastructure mean neglect for important security concepts?
- Understanding why it is more essential to focus on security when developing and deploying serverless applications
- Diving into the important questions if you're going serverless
- Demonstrating what an insecure serverless environment looks like, including how quickly a small vulnerability can lead to huge data loss

BULLETPROOF

9:45 am - 10:20 am

WORKSHOP
BREAKOUT ROOM 2

It's Time to Rethink Network Security for Cloud

- Cloud architects, CIOs and CISOs will learn how their peers are reducing the complexity and costs of network security in the cloud.
- Find out how enterprises are saving tens of thousands to millions of dollars annually by removing expensive licenses, compute, cloud data processing costs tied to using "Last Generation Firewall" architecture in the cloud.
- Learn how the convergence of cloud networking and network security brings policy inspection and enforcement into the natural path of traffic to improve performance, strengthen compliance, boost cyber resiliency, and accelerate cloud infrastructure automation projects.

aviatrix

Rod Stuhlmuller
VP Solutions Marketing
Aviatrix

Bryan Woodworth
Dir. Solution Strategy
Aviatrix

10:25 am - 12:05 pm

Pre-Arranged One-to-One Meetings

10:30 am – 10:50 am: Meeting Slot 1/Networking
10:55 am – 11:15 am: Meeting Slot 2/Networking
11:20 am – 11:40 am: Meeting Slot 3/Networking
11:45 am – 12:05 pm: Meeting Slot 4/Networking

AGENDA

12:10 pm - 12:45 pm

BREAKOUT ROOM 1
DATA MANAGEMENT

How Good Data Security Practices Drive Data Governance

- Exploring key strategies to enable effective data stewardship, support innovation, and automate compliance while moving at the speed of the cloud
- Gaining complete visibility into your data repositories
- Ensuring scalability as you continue to generate exponential volumes of data
- Implementing cloud-managed environments to handle innovations and new workloads

Kostas Georgakopoulos
Chief Technology Officer & Chief Information Security Officer
Mondelez International

12:10 pm - 12:45 pm

BREAKOUT ROOM 2
SECURITY STRATEGY

Why Should You Care About the Big Bad Threat Actors?

- Who is responsible for navigating cyber security in a digitally driven world?
- Exploring ways to create and sustain digital trust across your organization by making it everyone's business
- Understanding how the impacts of changing technology have far-reaching impacts on the integrity of your organisation
- The importance of connectivity: How your cyber team, c-suite and every employee need to work hand in hand to drive positive results

Sergio Torrontegui
Chief Business Information Security Officer, Americas
Unilever

12:45 pm - 1:45 pm **Overflow Lunch Seating**

12:45 pm - 1:45 pm **Themed Lunch Discussions**

Themed lunches are roundtable discussions on specific industry issues and challenges during lunch hour. Each roundtable will be led by a sponsor or delegate who is an expert in the field. Limited seating is available, so please sign up for your preferred topic through the event app. Choose one from:

Utilizing the New Generation of Robotics to Get Ahead

Phillip Arthur
VP Chief Technology Officer
AdventHealth

Cybersecurity and the Board: Strategies for Alignment

DeWayne Hixson
CISO
Bass Pro

AGENDA

Driving Real Value Through AppSec Processes and Tech

Jeremy Schumacher
SVP, IT & Security
Cadent, LLC

Innovate, Integrate, Influence: Tools for Effective Leadership

Mike Phillips
CISO
Cheniere Energy

How To Implement Data Governance In The Consumer Space

Ashiq Ahamed
Global CIO
Destination Auto Group

How to Maximize ICS to Boost Efficiency and Data Management

Joseph Welch
Chief Information Officer
Fort Wayne City Utilities

Cybersecurity at the Nexus of AI and Automation

Leo Howell
Interim Vice President of Information Technology and Chief Information Officer
Georgia Tech

What Should We Take Away From Recent SEC Decisions Regarding CISOs?

Metrics and Measuring Success

Jim Blevins
CIO
Richwood Bank

AGENDA

1:45 pm - 2:20 pm

Building Cyber Resilience in a Cyber-Physical World

- **Understanding the Five Pillars of Cyber Resilience:** Begin by delving into the five fundamental pillars of cyber resilience: Prevention, Detection, Response, Recovery, and Adaptation. Explain how each pillar plays a crucial role in fortifying systems against cyber threats in a cyber-physical environment. Emphasize the interconnectedness of these pillars and how they form the foundation of a robust cyber resilience strategy
- **Assessing Vulnerabilities in Cyber-Physical Systems:** Explore the unique challenges posed by cyber-physical systems, where digital and physical components are deeply intertwined. Discuss how vulnerabilities in these systems can have real-world consequences, from disrupting critical infrastructure to endangering human safety. Highlight the importance of conducting thorough risk assessments to identify potential weak points and prioritize mitigation efforts
- **Implementing Multilayered Defense Mechanisms:** Dive into strategies for building resilient systems and infrastructure by employing multilayered defense mechanisms. Discuss the importance of combining technical controls (such as encryption, firewalls, and intrusion detection systems) with human-centric approaches (such as cybersecurity training and incident response planning). Illustrate how a layered defense approach can provide comprehensive protection against evolving cyber threats
- **Developing Incident Response and Recovery Plans:** Outline the process of developing and executing incident response and recovery plans tailored to the unique challenges of cyber-physical systems. Discuss the importance of establishing clear protocols for detecting and responding to cyber incidents promptly. Highlight the role of collaboration among stakeholders, including IT professionals, operational teams, and management, in effectively mitigating the impact of cyber attacks and restoring normal operations

Taylor Lehmann
Director, Office of the CISO
Google

2:25 pm - 3:00 pm

WORKSHOP
BREAKOUT ROOM 1

Redefining DevSecOps After SolarWinds: Lessons from a Securities Lawyer Turned Cyber Hacker

In this practical workshop, CISOs will learn from real world lessons and come away with a better understanding of:

- The real meaning of SolarWinds and the SEC's 4-day rule
- How to define an "incident" for disclosure and remediation
- Is there a remediation safe harbor?
- The CISOs role in cyber disclosure do's and don'ts
- Using technology to claim control over cyber delivery

Tom Tovar
Co-founder & CEO
Appdome

AGENDA

2:25 pm - 3:00 pm

WORKSHOP
BREAKOUT ROOM 2

'Shift up' observability of your custom software security risks and beyond

Overwhelming complexity in custom software results in costly data breaches with open source and 3rd party component vulnerabilities like the log4j incident being a major culprit. Software Composition Analysis (SCA) technology is designed to help reduce these risks. However, most traditional SCA products are designed for developers and don't give CISOs and CIOs the visibility they need to confidently make critical decisions and take control of open source and 3rd party component risks across their entire portfolio of software applications. How do you ensure you are covering all of your applications? How do you govern these risks without slowing down your developers?

Complexity is so high, it's no longer good enough to rely solely on developers to be vigilant. Join this session to learn how some CISOs and CIOs are taking a smarter approach to open source and 3rd party component security risk management by 'shifting up' observability with an open source control tower, automatically across all their applications. Get answers to questions like:

- Do I have new security or IP exposures this month?
- Are risky components, like log4j, still being used?
- Who exactly is using the custom framework we built and where?
- How do I ensure I am ready for Software Bill of Materials (SBOM) requirements and regulations?

CAST
Software Intelligence for Digital Leaders

Greg Rivera
VP of Product
CAST Software

3:05 pm - 4:15 pm

Pre-Arranged One-to-One Meetings

3:05 pm – 3:25 pm: Meeting Slot 5/Networking
3:30 pm – 3:50 pm: Meeting Slot 6/Networking
3:55 pm – 4:15 pm: Meeting Slot 7/Networking

3:40 pm - 4:15 pm

Focus Group

Focus group is informal moderated conversations among peers that occur during networking time outside the regularly scheduled conference agenda. There is no sign up. Delegates and speakers are welcome to opt into any focus group that interests them. The focus group will take place in the corners of the Exhibition Hall in well-marked areas that include a sound barrier. All participants will be provided with wireless headphones to ensure everything said can be heard over the background noise of the Exhibition Hall.

The Hybrid Office and Cyber Security Protection in the New Normal

MARS

Andrew Stanley
CISO & VP Global Digital Operations
MARS

AGENDA

4:20 pm - 4:55 pm

BREAKOUT ROOM 1
DATA MANAGEMENT

New Data Governance and Cyber Resiliency Standards for Healthcare

- Exploring why traditional vulnerability management approaches are limited in effectiveness in healthcare organizations
- Strategies for establishing standardized baseline cybersecurity controls to protect patient data and care
- Understanding the landscape of healthcare's attack ecosystem and highlighting some of the common pitfalls

Arve Kjoelen
CISO
McAfee

4:20 pm - 4:55 pm

BREAKOUT ROOM 2
SECURITY STRATEGY

Why Your Cyber Resilience Strategy Should Be Intelligence-Led

- Designing a holistic and pragmatic cyber resiliency strategy to manage cyber risk and drive business value
- How to develop your strategy to ensure it is aligned with your business strategy
- Incorporating key aspects such as legal, compliance, and risk management to enable a return on investment
- Discussing how intelligence and the frontline experience should be leveraged within your organization

Cynthia Kaiser
Deputy Assistant Director, Cyber Division
Federal Bureau of Investigation (FBI)

4:55 pm - 5:30 pm

Prevent, Detect, and Respond: Finding and Fixing Flaws

- Why increased security sometimes starts with developer competency in a developing environment or a growth period
- Exploring ways of managing and maintaining your attack surface
- Learning from actionable, practical response processes from major organizations that have been there, done that, and come out on the other side

Gary Harbison
Global Chief Information Security Officer
Johnson & Johnson

AGENDA

5:30 pm - 6:05 pm

Achieving a Dominant Cybersecurity Posture in the Digital Economy

- Digital Transformation as an imperative to protect the homeland from the nation's adversaries
- Accelerating cloud migration to enhance war fighting effectiveness
- Deploying a high-degree of automation to improve defensive capabilities across agencies
- Zero Trust adoption as a federal priority and its implications for the industry at large

David McKeown
Deputy DoD CIO for Cybersecurity/
Chief Information Security Officer
United States Department of Defense

6:05 pm - 6:10 pm

Chair's Closing Address

Tomás Maldonado
Chief Information
Security Officer
National Football League

6:10 pm - 7:10 pm

JUNE 18, 2024

7:30 am - 8:30 am

Registration and Breakfast

7:45 am - 8:30 am

BREAKFAST WORKSHOP

BREAKOUT ROOM 2

Combating Data Loss and Insider Risk

- Moving beyond legacy data loss prevention approaches
- Managing insider threats and risks in your organization
- Increasing visibility across multiple channels to accelerate incident response

AGENDA

8:30 am - 8:35 am

Chair's Welcome Remarks

Tomás Maldonado
Chief Information Security Officer
National Football League

8:35 am - 9:10 am

Managing Your Insider Risk Program

- Emphasizing the balance between employee privacy and company security
- Prioritizing collaboration across functions and the importance of shared goals with clear measures of success
- Engaging employees with data protection and compliance training
- Utilizing emerging new insider risk management tools with adaptive security capabilities that can detect risky activities and mitigate potential impact

Bret Arsenault
Corporate Vice President and Chief Cybersecurity Advisor, Microsoft
Microsoft

9:10 am - 9:45 am

Security in the Open: How to Raise the Bar on Open Source Software Security

- Working upstream to improve long-term outcomes
- Releasing security tools and libraries as open source to help secure the broader ecosystem
- Providing engineering and financial support for security improvements across the ecosystem
- Some reflections on software supply chain, secure software development, and memory-safe languages

Mark Ryland
Director, Amazon Security
Amazon

ROOM 1 CHAIR

Tomás Maldonado
Chief Information Security Officer
National Football League

ROOM 2 CHAIR

TBA

AGENDA

9:50 am - 10:25 am

BREAKOUT ROOM 1
DATA MANAGEMENT

Fireside Chat: The Best Security Offense is a Good Defense

- Guarding potential new attack surfaces caused by growing digitization across operations
- Exploring emerging concerns around attacks enabled by the growing availability of generative AI tools
- Collaborating with everyone at the national, state, and local levels to test and trial scenarios leading up to a national event to ensure preparation
- Constantly focusing on maximizing visibility and assessing threats
- Working towards maximum visibility into networks and creating multiple layers of defense

Tomás Maldonado
Chief Information Security Officer
National Football League

9:50 am - 10:25 am

BREAKOUT ROOM 2
SECURITY STRATEGY

Governing Generative AI: Safeguarding the Enterprise Without Stifling Exploration

- Identify and engage key stakeholders which may include developers, researchers, policymakers, ethicists, legal experts, affected communities, and end-users
- Establish risk tolerance through a policy with clear objectives and guiding principles guide the development, deployment, and use of generative AI systems
- Implement mechanisms for monitoring, auditing, and enforcing compliance with established policies and promote accountability
- Provide education and training to enhance understanding of generative AI technologies, governance principles, and ethical considerations among stakeholders.

Jeff Northrop
Chief Information Officer,
Mars Wrigley NA
Mars Inc

10:25 am - 11:15 am

Pre-Arranged One-to-One Meetings

10:30 am – 10:50 am: Meeting Slot 8/Networking
10:55 am – 11:15 am: Meeting Slot 9/Networking

AGENDA

10:40 am - 11:15 am **Focus Group**

Focus groups are informal moderated conversations among peers that occur during networking time outside the regularly scheduled conference agenda. There is no sign up. Delegates and speakers are welcome to opt into any focus group that interests them. The focus groups will take place in the corners of the Exhibition Hall in well-marked areas that include a sound barrier. All participants will be provided with wireless headphones to ensure everything said can be heard over the background noise of the Exhibition Hall.

Clean Room as a Service

Microsoft

Dr. Tyrone Grandison
Chief Technology Officer – App Innovation, Infrastructure, and Security – GISVs & Digital Natives
Microsoft

Startups Unveiled: Adding Value to Your Stack

Community Veterinary Partners
the pet people people™

Andrew Wilder
Chief Security Officer
Community Veterinary Partners

11:20 am - 11:55 am

WORKSHOP
BREAKOUT ROOM 1

Never Let a Good Crisis Go to Waste: A Ransomware Case Study

- Highlighting the importance of designating key decision-makers for handling crises before they happen
- Getting comfortable making critical decisions during a ransomware attack without a lot of data
- How a crisis allowed for more effective implementation of security changes

11:20 am - 11:55 am

WORKSHOP
BREAKOUT ROOM 2

Driving Real Value Through AppSec Processes and Tech

- Dissecting the efficacy of tools like SAST, DAST, and SCA; or processes like Threat Modeling and Pen Testing
- Addressing issues with these tools and processes through thoughtful exchange and actionable insights
- Challenging assumptions regarding long-accepted processes
- Sharing perspectives and gathering understanding through the experiences of CISOs

AGENDA

12:00 pm - 12:35 pm

Defending Global Institutions from Supply Chain Cyber Risks

- Learning how supply chain cyber risks pose unacceptable risk levels to supply chain operations to the and how we can proactively mitigate
- Gaining a better understanding of both short and long term impacts that supply chain cyber risks pose across the value chain
- Taking a deep dive into real-world data to understand the magnitude of potential issues and how vulnerable some of the most critical industries are

Gene Sun
Corporate Vice President, Chief Information Security Officer and Risk Management
FedEx Corporation

12:35 pm - 1:35 pm

Overflow Lunch Seating

12:35 pm - 1:35 pm

Themed Lunch Discussions

Themed lunches are roundtable discussions on specific industry issues and challenges during lunch hour. Each roundtable will be led by a sponsor or delegate who is an expert in the field. Limited seating is available, so please sign up for your preferred topic through the event app. Choose one from:

Security Concerns for CISOs and How to Address Them

Josh Serba
Chief Information Officer
AHC+ Hospitality

Lessons Learned: Failing Forward

Rick Rampersad
Chief Information Officer
Early Learning Coalition of Hillsborough County

Securing the Resources You Need to Succeed in a Crowded and Noisy Business Environment

Brandon Carter
Sr. Cybersecurity Specialist
Environmental Protection Agency

Reinvigorating Long-Established and Too Comfortable Processes, Protocols, and Procedures

David Mullenix
Vice President, IT
JPI

AGENDA

Cybersecurity in a High-Churn Workforce

Andrew Cook
Senior Manager of IT Security & Infrastructure
Milos Tea Company

Cybersecurity for the Mid-market Organization

Tom Shock
Director, Information Technology
Shepherd Electric Supply

Managing Cyber Risk in Distributed Environments – Leading Through Influence, Policy, and Collaboration Based Approaches

Jessie Minton
VC and CIO
Washington University in St. Louis

Challenges of Adversarial AI in Cybersecurity

Omar Valerio
CIO / CTO
Westminster Christian School

Bringing NOC Optimization Best Practices to SOC Working Environments

1:35 pm - 2:10 pm

Network-Embedded Security: Securing Connections for Everyone

- How AT&T is using advanced cybersecurity services that are embedded into the network to combat the rising number of cyber-attacks
- Why network-embedded security offers a more robust defense by actively detecting and mitigating threats faster and more effectively than many options available today
- Discussing how businesses small to large can be thinking about their cyber defenses in the future

Rich Baich
SVP, Chief Information Security Officer
AT&T

AGENDA

2:15 pm - 2:50 pm

Panel: The Business of Global Talent

- Placing diversity and inclusivity at the core of everything you do
- Breaking new ground and finding new ways of managing the holistic talent life cycle, enabled by advanced technology
- Forging partnerships across the business to attract a new generation of talent from outside the core cyber function
- Using internal, external and unconventional talent pools to build and develop a sustainable global talent pipeline

Moderator:

Tomás Maldonado
Chief Information Security Officer
National Football League

Panelists:

Eddie Borrero
VP & CISO
Blue Shield California

Andrew Albrecht
Vice President – Chief Information Security Officer (CISO)
Domino's

Eric Smith
VP, US CISO
TD Bank

Matt Conner
Chief Information Security Officer
Westinghouse Electric Corporation

2:55 pm - 3:00 pm

Chair's Closing Remarks

Tomás Maldonado
Chief Information Security Officer
National Football League