C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CIO/CISO Think Tank

SPEAKERS

Lee Painter
Global Head of Information Security Governance
Zurich Insurance Group

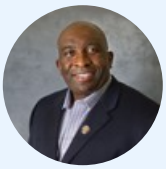
Jason Lewkowicz
SVP Cyber Defense & Applied Security
Optiv

John Kellerhals
Security Operations Manager
CF Industries Holdings

Richard Rushing
CISO
Lenovo

Michael Gross
Cybersecurity Manager
Cleveland Clinic

John Tryon
Head- Information Security
Health Care Service Corporation

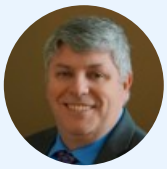


Calvin Nobles Ph.D.
Chair Information Technology & Management
Illinois Institute of Technology

Sean Boulter
Principal Security Engineer, US North Central
Salt Security

Steve Zalewski
Former CISO
Levi Strauss & Co.

Brad Thies
Founder and President
BARR Advisory



Ken Kazinski
Cyber Security - Attack Surface Management
Abbott Laboratories

Steve Rubinow
Director Institute for Professional Development - Computing & Digital Media
DePaul University Jarvis College of Computing and Digital Media

Michael Gross
CEO
Engrossed Advisory

John Tryon
CISO
CONMED Corporation

Click Here to Register

June 02, 2022

Central Time

Registration & Networking Lunch

12:30 PM-1:30 PM

Welcome

1:30 PM-1:40 PM

KEYNOTE PANEL
Zero Trust Network

1:40 PM-2:35 PM

A zero trust approach to security has been steadily gaining steam for the last several years. The importance of this approach reached a new level with the May 2021 White House executive order requiring federal agencies to shift to this architecture by fall 2024. Ransomware continues to grow and clearly as remote work became the new norm, and e-commerce increased. Leaders need to establish a mature level of cyber resilience to better handle ransomware and other potential data breaches. Luckily, zero trust can play a critical part in that strategy as more and more businesses are realizing that to build customer trust they must establish zero tolerance for trust in their security strategy. Will Zero Tolerance for Trust redefine the state of security as government and private industry scrutinize their trusted relationships more, and re-evaluate the 'who, what, why' in 2022 more than any other year?

CHAIR

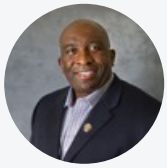
Steve Zalewski
Former CISO
Levi Strauss & Co.

PANELISTS

Richard Rushing
CISO
Lenovo

John Tryon
Head- Information Security
Health Care Service Corporation

Lee Painter
Global Head of Information Security Governance
Zurich Insurance Group



Calvin Nobles Ph.D.
Chair Information Technology & Management
Illinois Institute of Technology

Networking Break

2:35 PM-2:50 PM

FIRESIDE CHAT
What's AI Doing for You?

2:50 PM-3:35 PM

The terms "Artificial Intelligence" and "Advanced Machine Learning" are often thought of interchangeably. While there is a relationship between AI and AML, to say they are the same thing is an oversimplification and misclassification. Rather, one begets the other with AI being the basic principle upon which AML is developed. As AI begins to mature and migrate away from purely advanced mathematical operations into decision making paradigms, AML steps forward as the predictive ability of machines to process vast quantities of data. As

data and analytics becomes foundational to the way every business operates, AI and AML will become foundational capabilities.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Co.

PANELISTS

John Kellerhals
Security Operations Manager
CF Industries Holdings

Steve Rubinow
Director Institute for Professional Development - Computing & Digital Media
DePaul University Jarvis College of Computing and Digital Media

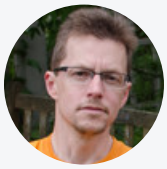
DISRUPTOR

The Explosion of API Security

3:40 PM-3:55 PM

How do CISOs get the most out of APIs while limiting the risk? 20 years ago the motives for hackers were website defacement and getting your name on all those defacements. That was the point of hacking. Now, it's all about monetizing the data you can steal. Just as cloud computing initially seeped into organizations under the cloak of shadow IT, application programming interface (API) adoption has often followed an organic, inexact, and unaudited path. IT leaders know they are benefiting from APIs, internal, via third parties, and often outwardly exposed. They just don't know where they are, how much they support key services, and how they're being used, or abused! In this session we will discuss if APIs are meant to be exposed, and discuss if the startups API software companies are ready for the explosion.

PANELISTS



Sean Boulter
Principal Security Engineer, US North Central
Salt Security

Networking Break

3:55 PM-4:10 PM

DISRUPTOR

Building Trust and Resilience Through Cloud Security and Compliance

4:10 PM-4:25 PM

With a mass migration to the cloud due to the ongoing pandemic, now is the perfect time to talk about cloud security and compliance. For organizations in every industry, the cloud is now omnipresent, and therefore, security is paramount. We'll discuss the balancing act between security and compliance and explore how when security comes first, compliance follows. By understanding what goes into a successful cloud security program, how to implement those strategies and—most importantly and distinctively—how to use security and compliance as a differentiator, organizations will build trust with their clients, create cybersecurity resilience, and boost their brand.

PANELISTS

Brad Thies
Founder and President
BARR Advisory

PANEL
Guarding the Doors: Navigating 3rd Party Risk

4:30 PM-5:25 PM

As organizations expand their third-party ecosystem, many are challenged with executing core activities that are critical to operations, risk profiles, and compliance posture without compromising the quality of data collection, evaluation, and mitigation measures increasingly outsourcing business activities to 3rd-party vendors. It is critical for an organization to be vigilant when selecting the right 3rd-party vendor with the appropriate security posture, as many vendors are hosting, processing and transmitting sensitive regulatory information with unrestrained access to our IT assets. At the highest level, third-party incidents can result in reputational damage, non-compliance, or even criminal activity, which can negatively impact earnings and shareholder value. To address this challenge, many organizations are investing in technology to support vendor risk management. Technology isn't the entire answer to managing third-party risk, however the right technology or collection of technologies, coupled with optimal processes, can enable organizations to bridge the gap.

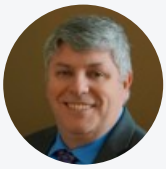
CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Co.

PANELISTS

Jason Lewkowicz
SVP Cyber Defense & Applied Security
Optiv

Michael Gross
Cybersecurity Manager
Cleveland Clinic



Ken Kazinski
Cyber Security - Attack Surface Management
Abbott Laboratories

Closing Remarks

5:25 PM-5:30 PM

Cocktail Hour

5:30 PM-6:30 PM

TOGETHER WITH

SALT BARR ADVISORY

SafeBreach zscaler cynet