C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

Cybersecurity Think Tank

SPEAKERS



Frank Schmahlenberger
CISO
Cathay Bank



Dan Meacham
CSO, CISO
Legendary Entertainment



Wilson Ye
CISO
Loeb & Loeb LLP



Joseph Zhou
Americas CISO
Shein



Premkumar Thomas Augustine
VP, Engineering Services & CISO
Finvi



Andrei Bostan
Director, Cybersecurity Risk
Bank of Hope

Click Here to Register

April 20, 2027

Pacific 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

29 Minutes in Los Angeles. Who Gets to Act Before the Attacker Does?

9:40 AM-10:05 AM

The average attacker now moves from a first foothold to the rest of the network in about 29 minutes. In a region home to the nation's busiest port complex, major health systems, community banks and global online retailers, an hour offline is measured in containers, patients and orders. Yet in many organizations the decision to isolate a system, cut a supplier connection or take a revenue platform offline still waits for a meeting and an executive who may be on a plane.

This opening keynote looks at the human side of speed. Who holds the authority to act in the first half hour, what they are allowed to break without asking, and how leading CISOs agree those decision rights with the CEO, the business and the board long before the night they are needed. The fastest response, it turns out, is the decision that was already made.

PANEL

Logged In, Cleaned Out. Stopping Account Takeover Across Commerce and Banking.

10:10 AM-10:55 AM

For many organizations the most damaging attacks no longer target the company at all. They target its customers. Stolen passwords, hijacked sessions, convincing fake support calls and AI written phishing let criminals walk into real accounts, drain balances, redirect orders and leave the brand to absorb the anger and the losses.

This panel brings together security and fraud leaders from banking, retail and digital commerce to compare how they protect customer accounts without driving customers away. How to spot a takeover in progress, where stronger sign in methods are finally winning, how security and fraud teams can work as one, and how to talk to customers honestly when something goes wrong.

Coffee Break

10:55 AM-11:15 AM

VISION VOICES

The Browser Grew Hands. What to Know Before AI Starts Clicking, Typing and Buying for Your People.

11:15 AM-11:30 AM

The browser used to be a window. Now it is becoming a worker. AI browsers and assistants can read a page, fill in a form, approve a request and complete a purchase on someone's behalf, and a single hidden instruction tucked inside a web page can redirect all of it. In fifteen focused minutes, this session explains why the browser has become one of the most important places to defend, what prompt injection looks like when it meets real credentials, and which simple policies let your people enjoy the help without handing the keys to whoever wrote the page.

PANEL

11:35 AM-12:20 PM

Who Signs Off in California? Cyber Audits, Insurance and Accountability Under the New Privacy Rules.

California has raised the bar for proving security, not just promising it. New rules from the state's privacy agency took effect in January 2026. Larger businesses must complete their first independent cybersecurity audit, covering 2027, and certify it by April 2028, while rules on automated decisionmaking apply from January 2027. At the same time, insurers are asking sharper questions at renewal. How many AI agents run in your environment? Who approved their permissions? Can you prove a human signed off on that payment? This panel brings together security leaders, risk owners and the people who underwrite them for a frank conversation about audits, coverage and accountability in the age of autonomous systems. Leave knowing what your auditor and your carrier will ask next, what your AI vendor contracts should say, and how to make sure the fine print protects you rather than surprises you.

Lunch

12:20 PM-1:20 PM

VISION VOICES

1:25 PM-1:45 PM

Think Like the Attacker. Why Southern California Security Leaders Are Investing in Offense Again.

For a long time, offensive security meant the annual penetration test, a thick report and a list of findings that was already out of date by the time anyone read it. AI has changed the economics on both sides. The tools attackers use to probe your defenses around the clock are now in your hands too, and security leaders are investing in offense again with real urgency.
This session explores continuous, AI assisted red teaming. What it finds that traditional testing misses, how to run it safely against live systems, and how to turn a constant stream of findings into fixes instead of fatigue.

DISRUPTOR

1:50 PM-2:05 PM

Who Built Your AI? Mapping the New Supply Chain Behind Every Model You Use.

Third party risk used to mean vendors, contractors and the software they shipped. Today it also means the foundation models you call, the open weights your developers download, the plugins and connectors your agents rely on, and the data those models learned from. Each one is a link in a chain you did not forge yourself.
This disruptor session maps the new AI supply chain and shows how to inventory it, assess it and set sensible guardrails without bringing innovation to a halt.

PANEL

2:10 PM-2:55 PM

Gateway to the Pacific. When World Events Reach Southern California Networks.

Southern California is where much of America meets the Pacific. Cargo moves through its ports, data moves through subsea cables that land along its coast, and its companies run teams, suppliers, data centers and customers across the world. A regional outage, damage to a subsea cable, a disruption at a key supplier, a sudden change in data rules or a wave of attacks aimed at one industry can travel across the ocean and arrive in your logs before the morning news has caught up.
This panel helps security leaders see further. How to build threat intelligence that reflects where you actually operate, how to plan for the loss of a key supplier or region, and how to brief a board that wants to understand global risk in plain business terms. It is a conversation about preparation, so your organization is never the last to know.

Networking Break

2:55 PM-3:15 PM

VISION VOICES

3:15 PM-3:30 PM

No Encryption Required. When Extortion Skips the Ransomware Entirely.

For years the defense against ransomware was simple to explain. Keep good backups and you will never have to pay. Many criminal groups have adapted. They no longer bother to lock your systems. They copy your data, then threaten to publish it, contact your customers or alert your regulators, and no backup in the world makes that threat go away.
This short session looks at the rise of pure data extortion and what it changes for leaders. Where data protection matters more than recovery, how to learn quickly what was actually taken, and how to prepare communications for customers and regulators before the first message from the attackers arrives.

FIRESIDE CHAT

3:35 PM-4:10 PM

What I Wish I Had Known. Security Leaders on the Decisions That Shaped Them.

Every CISO carries a private library of moments. The breach that taught humility, the board meeting that changed how they speak, the hire that transformed a team, the warning they ignored once and never again. These stories rarely make it onto conference slides, yet they are where real wisdom lives.
This closing fireside invites seasoned security leaders to open that library. Honest, warm and practical, it is the conversation you usually only have late at night after an event, offered here to everyone in the room, especially those still writing the first chapters of their own careers.

Closing Remarks & Raffle Giveaway

4:10 PM-4:20 PM

Cocktail Reception

4:20 PM-5:30 PM

PARTNERS

We are currently accepting partnership opportunities for this event.