C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

Cybersecurity Think Tank

SPEAKERS



Sue Bergamo
CIO & CISO
BTE Partners



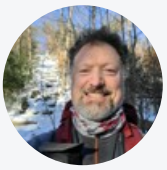
Melissa Ouari
VP & CISO
Money Management International



Jim Haynie
CIO/CISO
New England IT Security Consortium



Wes Kussmaul
CISO
Authenticity Institute



Michael Meyer
vCISO
Highlight Technologies



Nawar Faruque
Head of IS Governance, Risk & Compliance
Genetix Biotherapeutics

Click Here to Register

May 05, 2027

Eastern 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

9:40 AM-10:05 AM

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

The average attacker now moves from a first foothold to the rest of the network in about 29 minutes. In a region built on hospitals, research labs, universities and the firms that manage trillions of dollars for investors around the world, an hour offline is measured in patients, experiments and trades. 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

10:10 AM-10:55 AM

Hire, Badge, Retire. Running the Full Employee Lifecycle for AI Agents.

We spent twenty years learning how to trust people with access. We screen them, onboard them, give them only what they need, review their work and collect the badge on their last day. AI agents are now joining the workforce, often hired by a business unit that forgot to tell security, and most of them never go through any of those steps.
This panel borrows the employee lifecycle and applies it to digital workers, one stage at a time. Who approves the hire, how an agent gets its badge and its manager, what a performance review looks like for software, and how to retire an agent cleanly so its access does not outlive its purpose. Expect honest stories, the controls that held up, and the ones that did not.

Coffee Break

10:55 AM-11:15 AM

VISION VOICES

11:15 AM-11:30 AM

The Browser Grew Hands. Securing AI Browsers That Click, Type and Buy for Your People.

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 Pays When the Agent Gets It Wrong? Cyber Insurance, Liability and the Massachusetts Rulebook.

Insurers read the same headlines you do, and the questions on renewal forms are changing quickly. How many AI agents run in your environment? Who signed off on their permissions? Can you prove a human approved that payment? Massachusetts adds its own layer. For more than fifteen years the state has required companies that hold residents' personal information to keep a written security program, and lawmakers on Beacon Hill have spent the past year working on one of the most ambitious consumer privacy bills in the country.

This panel brings together security leaders, risk owners and the people who underwrite them for a frank conversation about coverage, exclusions and accountability in the age of autonomous systems. Leave knowing what 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 Boston 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

Your Supply Chain Now Has a Model in It.

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

Guarding the Breakthrough. Research Security for Labs, Hospitals and the Companies Around Them.

2:10 PM-2:55 PM

Boston is one of the world's great engines of discovery. Early research on new treatments, clinical trial data, genomic discoveries, robotics designs and the investment strategies built around them all live on networks in and around this city, and that makes them a prize for criminal groups and state backed spies alike. A single stolen dataset can erase years of work and a competitive lead worth billions.

This panel helps security leaders protect the ideas that matter most. How to build threat intelligence that reflects who is really targeting your research, how to secure open, collaborative environments without slowing the scientists down, how to manage partners and universities across borders, and how to brief a board that wants to understand the risk in plain business terms.

Networking Break

2:55 PM-3:15 PM

VISION VOICES

No Encryption Required. When Extortion Skips the Ransomware Entirely.

3:15 PM-3:30 PM

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. For hospitals, universities and research labs holding patient records and student files, the harm is deeply personal.

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 patients, customers and regulators before the first message from the attackers arrives.

FIRESIDE CHAT

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

3:35 PM-4:10 PM

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.