

PANEL DISCUSSION

Cyber Breach Response Under Fire

What CISOs, Legal Leaders, and Boards Get Wrong
in the First 72 Hours

CISO NY Conference | Hoboken, New Jersey
September 24, 2026



Panelists



Corey Dennis

Chief Privacy Officer &
Assistant General Counsel

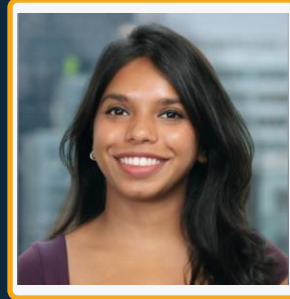
LEGEND BIOTECH



Jim Rutt

Chief Information Officer

DANA FOUNDATION



Shivani Suresh

Assistant Vice President,
Information Security Engineer

SYNCHRONY



Donna Ross

Chief Information Security
Officer

RADIAN



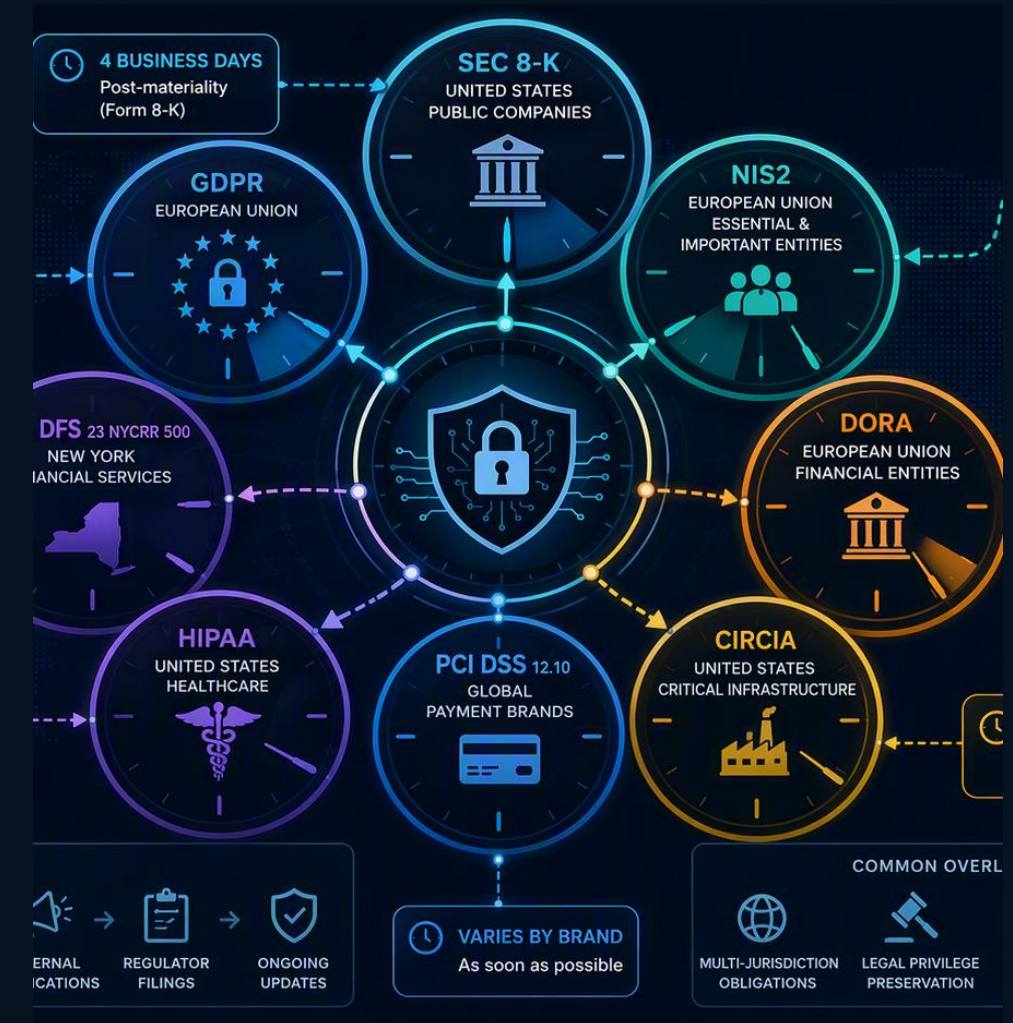
Stephen Garcia

Chief Information Security
Officer

BREACHRX

The Legal Clock Starts Before the Facts Are Complete

U.S. STATE	Trigger varies by law	Individual and regulator notices follow jurisdiction-specific triggers and timelines.
SEC	Material incident	Form 8-K due 4 business days after materiality is determined.
GDPR	Personal data breach	Notify the authority within 72 hours unless unlikely to risk rights and freedoms.
NIS2	Significant incident	24-hour early warning, 72-hour notification, then final reporting.



Run legal, regulatory, insurance, and investigative workstreams in parallel.

The First 72 Hours: Decisions That Change the Outcome

1

Establish control

Name one incident commander and separate technical containment from legal and business decisions.

2

Protect the record

Engage counsel early, define forensic scope, preserve evidence and maintain decision logs.

3

Decide with incomplete facts

Use pre-agreed thresholds for shutdowns, materiality, notifications and escalation.

4

Align Security + Legal

Translate technical facts into business impact, legal triggers and defensible statements.

The first 24 hours are critical, but defensible decisions and coordinated execution must continue across the full 72 -hour window.

Do Not Outsource Accountability

FORENSICS

Define the question, preserve chain of custody and request evidence, not just conclusions.

VENDOR INCIDENTS

Demand scope, timeline and artifacts. Independently assess notification duties.

INSURANCE

Notify promptly and confirm panel counsel and forensic requirements.

COMMUNICATIONS

Use one fact base across regulators, customers, employees, the board and the public.



The forensic report informs the decision. It does not make the legal decision.

AI Changes the Tempo, Not the Accountability



ATTACKERS

- Faster social engineering and deepfakes
- Scaled vulnerability discovery and exploit development
- More persuasive business email compromise

DEFENDERS

- Faster triage, anomaly detection and containment
- Support for notification mapping and draft communications
- Better synthesis, but human validation remains essential

Board takeaway: speed without governance creates a second incident.