BREACHRX

DATA SHEET

Cybersecurity Incident Response Management Warranty

Up to $3 Million in Liability Protection

Personal and Corporate Protection for Security Leaders when Incidents Become Investigations

Cyber incidents increasingly trigger regulatory investigations, government inquiries, and scrutiny of individual decision-making. CISOs and senior executives are being named in actions, questioned about disclosure timing and oversight, and forced to defend their response under intense examination. When decisions made during an incident are questioned, your reputation and personal financial security are on the line.

BreachRx is the pioneer of Cybersecurity Incident Response Management (CIRM), and is now offers the first CIRM product backed by a contractual financial warranty, designed to protect both security leaders and business executives when cyber events escalate into regulatory, governmental scrutiny, or civil liability. It combines documented, defensible execution with meaningful financial protection.

Warranty Protection at a Glance

- **Up to $3 million per claim:** Financial protection for incidents managed through the BreachRx platform
- **Personal and Corporate Liability Protection:** Coverage for defense costs, fines, penalties, and negligence-related claims.
- **Zero Retention:** Applies without a retention requirement before coverage begins.
- **Executive Coverage:** CISOs, CEOs, General Counsel, and employees personally named in government or regulatory actions.
- **Fills Gaps in Cyber Insurance:** Covers financial exposure that fall below or outside existing insurance policies.
- **Global Insurance Partners:** Underwritten by global companies with financial strength.

For Security Leaders, the Risk is Now Personal

Regulators increasingly examine executives and not just companies. In today's enforcement environment, incident response decisions are scrutinized at the executive level, and security leaders are expected to demonstrate not only technical competence, but disciplined governance, timely escalation, and accurate disclosure judgment.

Security leaders face potential exposure from:

- SEC, FTC, and state regulatory investigations
- Alleged disclosure deficiencies
- Escalation or communication timelines
- Class-action customer lawsuits
- Claims or insufficient oversight of security operations or third-party risk
- Government inquiries tied to cyber incidents
- Negligence-related allegations questioning security governance

Corporate directors and officers' (D&O) coverage often does not protect security leaders. Policy exclusions, carve-outs, or allocation disputes can create uncertainty at precisely the moment financial assurance is needed. Indemnification is not always automatic, particularly if allegations involve misrepresentation or oversight failures. Defense costs begin on day one of any investigation before any determination of fault. This creates immediate personal financial pressure for the CISOs.

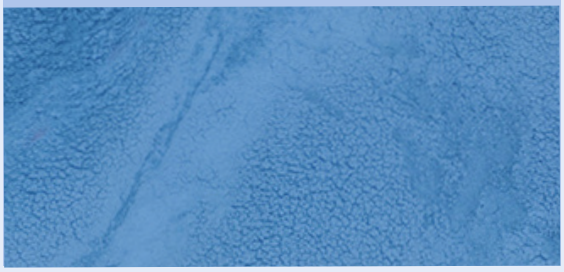
Financial Protection with Defensible Incident Response

When a cyber incident occurs, regulators and investigators do not simply evaluate the technical outcome but also the decision-making process.

- Was escalation timely?
- Were executives informed?
- Were disclosure decisions documented?
- Were legal obligations tracked and met?
- Can leadership demonstrate good-faith governance?

BreachRx CIRM transforms incident response from an ad hoc coordination effort into a structured, cross-functional, auditable enterprise-wide response. Security, legal, privacy, communications, IT, and executive leadership operate within defined workflows, documented decision points, timestamped actions, and privileged communication channels. The product creates a defensible record of how the organization responded: who knew what, when decisions were made, and how obligations were addressed.

If government or regulatory scrutiny follows despite documented good-faith adherence to disciplined execution within the CIRM product, the warranty provides financial protection for regulatory defense costs, fines and penalties, and negligence-related claims arising from the incident.



Built for Security Leaders Carrying Real Exposure

Today's Security Leaders operate in an environment where cyber risk is no longer just professional but also personal. They are expected to prevent incidents, manage crises flawlessly under pressure, brief the board with precision, and make disclosure judgments that may later be dissected by regulators, litigators, or prosecutors. Even when they act responsibly and in good faith, the possibility of being individually named or scrutinized is real.

BreachRx is designed to protect security leaders both ways — combining disciplined execution with meaningful financial protection

The BreachRx CIRM Warranty protects CISOs carrying that exposure by:

- Covering legal costs and fines for executives personally named in regulatory or governmental actions
- Addressing gaps where D&O insurance may have exclusions or coverage delays
- Cover defense costs during investigations, when legal expenses begin long before fault is determined.
- Applies from dollar one, without waiting for large retentions to be met.

Cyber incidents are operational events that test judgment, documentation, and credibility. BreachRx CIRM is designed to protect security leaders both ways — combining disciplined execution with meaningful financial protection

BREACHRX

AICPA SOC

SOC 2 Type II Certified

About Us

BreachRx offers the Rex Platform, an agentic AI-powered CIRM platform that orchestrates cross-functional incident response, guiding execution and ownership to enable faster containment and governance at enterprise scale.

Contact Us

info@breachrx.com
linkedin.com/company/breachrx
breachrx.com