

Defensibility.ai Opens Pre-Release of the Defensibility Gap Assessment Tool

Showing CISOs, TROs, GCs, CCOs, and CPOs Where Their Companies and Executives Are Legally Exposed Before Any Incident

SEATTLE, WA, UNITED STATES, June 22, 2026 /EINPresswire.com/ -- Defensibility.ai today opened



We don't promise immunity, and any vendor who does is selling you something. The platform documents what you're accountable for before any incident — so you can show you did your job."

John Johnson, Founder and CEO, Defensibility.ai

the pre-release of its [Defensibility Gap Assessment Tool](#) to a limited number of companies in exchange for feedback. The Tool is one of three products built on the company's Defensible Governance Framework; the other two are the [Defensible Governance application](#) and the [Minors Safety & Child Welfare application](#), both sold as annual subscriptions. Executives reserve access at defensibility.ai using a single role-based form and receive a complimentary 30-minute founder briefing tailored to their industry.

The Tool surfaces three things. The company's top regulatory exposure gaps — the unmet obligations that

would drive the most consequential fines if an enforcement matter arose tomorrow. Every C-suite executive's individual exposure, role by role — where the CEO, CFO, CISO, TRO, GC, CPO, and CRO each carry personal risk and where leadership accountability is undocumented. And the prosecutorial lens applied to those gaps — how a regulator, the FTC, the SEC, a state attorney general, or an EU supervisory authority would interpret the organization's posture and where they would build a case if asked.

Closing each gap — alternative safeguard review, CDAR risk thresholds, the remediation plan, and the sealed evidence record — is handled by the Defensible Governance application, not the Tool, which provides directional information on what closing each gap entails.

The Personal Defensibility Review — for CISOs and TROs

CISOs and TROs receive an additional layer: a Personal Defensibility Review, an in-product guided interview that produces a Job Record capturing the executive's current duties, responsibilities, accountability, mandate, and authority as the official job description with HR. It is designed to be signed inside the platform and saved as an evidentiary record.

The Review also produces a tailored personal plan beyond the Job Record — having their role named on the company's D&O policy, securing personal indemnification, ensuring their supervisor signs off on the documented job description, and identifying other protections that should be in place before any incident.

This layer exists because of the SolarWinds enforcement action. The SEC personally named Tim Brown, the company's Chief Information Security Officer, in October 2023 — the first time the SEC had personally named a sitting CISO in a cybersecurity enforcement matter. The agency voluntarily dismissed its case with prejudice in November 2025, more than two years after Brown was first named. Brown sits on Defensibility.ai's strategic advisory board and helped shape the Review around the documentation gaps the case exposed.

Founder and Advisor Quotes

"We don't promise immunity from enforcement, and any vendor who does is selling you something. What the platform provides is the infrastructure to document what you are and are not accountable for, the authority you've been given, the risks you've identified, the escalations you've made, the remediation you've recommended, and the funding you've requested — contemporaneously, before any incident. The point isn't to make any executive immune to scrutiny. The point is to ensure they can show they did their job."

— John Johnson, Founder and CEO, Defensibility.ai

"I'm not sure the SEC wouldn't still have tried to make an example of us. But it sure wouldn't have hurt to see if handing them that kind of record — that clarity about my role — would have been enough for them not to name me personally."

— Tim Brown, Strategic Advisor, Defensibility.ai (Chief Information Security Officer, SolarWinds; personally named by the SEC in 2023, case dismissed November 2025)

The Broader Enforcement Context

Personal liability for senior technology and security executives has shifted over the last three years. In October 2022, Joe Sullivan, formerly Chief Security Officer at Uber, was criminally convicted for obstruction of an FTC proceeding and misprision of felony in connection with concealing Uber's 2016 data breach. He was sentenced in May 2023 to three years of probation, 200 hours of community service, and a \$50,000 fine. The Ninth Circuit affirmed his conviction in March 2025 and later denied rehearing en banc.

In January 2023, the Federal Trade Commission finalized a consent order against the online alcohol marketplace Drizly and, personally, against its Chief Executive Officer James Cory Rellas, following a 2020 breach that exposed personal data of approximately 2.5 million consumers. Drizly and Rellas had been on notice of similar security problems since a 2018 incident, yet the FTC alleged that they failed to implement reasonable safeguards. The order personally binds

Rellas for 10 years to ensure that any qualifying future business where he is a majority owner, CEO, or senior officer with information-security responsibility maintains a formal information security program.

Company and Advisors

Defensibility.ai's two commercially available applications — the Defensible Governance application and the Minors Safety & Child Welfare application — are sold as annual subscriptions and are the subjects of pending U.S. provisional patent applications. The Defensible Governance application runs the full remediation workflow on the gaps surfaced by the Tool, including the sealed evidence record in the Evidence Locker. The Minors Safety & Child Welfare application applies the same Framework to platforms with minor users — gaming, social media, EdTech, and consumer platforms subject to the new psychological-welfare laws.

Defensibility.ai's strategic advisory board includes Tim Brown, the SolarWinds CISO personally named in the SEC's 2023 enforcement action; Rich Mason, former Global CSO/CISO of Honeywell; Wassil Kacha, former Global Head of Data Protection at Citi; Jeewon Kim Serrato, former Chief Privacy Officer of Fannie Mae and Berkeley Law privacy authority; John Kennedy, cybersecurity industry veteran with six patents; and Aleksandr Tiulkanov, an EU AI Act regulatory committee contributor.

Reservations for the Defensibility Gap Assessment Tool pre-release are open now at defensibility.ai.

About Defensibility.ai

Defensibility.ai builds the legal-defensibility layer for executive leadership and boards. Its three products are built on the company's Defensible Governance Framework, and the two applications are the subjects of pending U.S. provisional patent applications. The company does not guarantee any specific legal outcome and is not a replacement for legal advice from a licensed attorney. Visit defensibility.ai.

John Johnson

Defensibility.ai

john@defensibility.ai

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/921233263>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.