TAG

ANALYST REPORT

WHY CISOS MUST FOCUS ON NARRATIVE ATTACKS

DR. EDWARD AMOROSO, CEO TAG
WASIM KHALED, CEO BLACKBIRD AI

BLACKBIRD.AI

WHY CISOS MUST FOCUS ON NARRATIVE ATTACKS

EDWARD AMOROSO, CEO TAG
WASIM KHALED, CEO BLACKBIRD AI

Originally published in 2024, this updated edition reflects the rapid evolution of generative AI, agentic AI, large language models, synthetic media, and automated influence operations. While the central thesis remains unchanged – namely, that narrative attacks belong within the modern CISO's risk portfolio, the speed, scale, and sophistication of AI-enabled attacks have increased dramatically. This updated report explains why protecting digital trust has become a core element of enterprise cyber resilience.

INTRODUCTION

The modern Chief Information Security Officer (CISO) operates in an increasingly asymmetric threat environment. Adversaries need only identify one weakness, while defenders must protect enterprise systems, data, identities, brands, and digital trust. Security organizations have matured considerably during the past decade, but AI has fundamentally altered the offensive landscape.

Generative AI, multimodal models, voice cloning deepfakes, disinformation, misinformation, autonomous bots, and agentic AI now enable attackers to create persuasive narrative attack campaign at machine speed. These campaigns target organizations, executives, employees, investors, customers, and partners, making narrative security an emerging cybersecurity discipline rather than simply a communications issue.

WHAT IS A NARRATIVE ATTACK?

Narrative attacks created by the same threat actors, agenda driven influencers and nation states that create cyberattacks, use coordinated disinformation, misinformation and deepfake campaigns designed to manipulate perception rather than exploit software vulnerabilities. They blend truthful information with fabricated content to create significant reputational, trust, financial, cybersecurity's, physical and operational risk.

Modern narrative attack campaigns use AI-generated text, images, audio, video, fake websites, cloned executive voices, synthetic identities, and coordinated online personas that continually adapt based on audience engagement. The impact extends beyond public relations to customer confidence, employee morale, recruiting, investor sentiment, business partnerships, and even AI systems that consume public information.

For security leaders, coordinated narrative attack campaigns:

- Precede and amplify cyber incidents (it's the same threat actors)
- Target executives to do physical harm or reputational harm
- Undermine trust with customers, investors, and employees
- Cause brand reputational harm
- Enable insider threats
- Threaten supply chain, critical manufacturing & infrastructure
- Manipulate stock valuation
- Impact Due diligence / M&A / Corporate intelligence

HOW HAVE REPUTATIONS BEEN PROTECTED TRADITIONALLY?

Organizations have historically relied on public relations, legal teams, media monitoring, and social listening after damaging stories appeared online. These approaches were largely reactive and increasingly ineffective.

Modern AI-driven narrative attacks spread simultaneously at scale across multiple social media, news and dark web platforms and forums and often bypass traditional media. AI-powered narrative intelligence platforms can detect coordinated influence campaigns, identifies the threat actors, networks, bots, and communities driving them; and turns those signals into early warning, decision intelligence, and coordinated response. before false narratives become established.

THE ROLE OF THE CISO IN NARRATIVE ATTACKS

Historically, CISOs protected enterprise technology while communications teams managed reputation. That distinction is disappearing. Boards, regulators, customers, and executive leadership increasingly expect security leaders to protect digital trust alongside infrastructure.

Because AI-powered narrative attacks are highly automated and now threaten the company and executives, CISOs are well positioned to deploy AI-powered Narrative Intelligence Detection and Response technologies while coordinating with communications, legal, human resources, and executive leadership.

WHY AI CHANGES EVERYTHING

Our original 2024 edition anticipated that AI would dramatically increase the scale of narrative attacks. That prediction has become reality. Generative AI has reduced the cost of producing convincing disinformation, misinformation and deepfakes to almost zero, while agentic AI enables campaigns to operate continuously with minimal human oversight.

Multimodal AI now enables attackers to create convincing synthetic voices, realistic videos, fabricated executive interviews, cloned websites, and coordinated influence campaigns that are increasingly difficult to distinguish from authentic content.

Narrative attacks now influence both people and machines. Enterprise AI assistants and autonomous business agents consume public information as part of normal operations. Manipulating that information ecosystem can therefore affect business decisions as well as public perception.

The cybersecurity industry has historically answered automation with better automation. Narrative Intelligence security should follow the same path through AI-powered defensive platforms capable of continuously detecting, analyzing, and responding to coordinated influence campaigns.

ROLE OF THE CISO IN ADDRESSING THE GAP

Narrative Intelligence security should become an integral component of enterprise cyber risk management. Narrative Intelligence Detection and Response platforms such as Blackbird.AI demonstrate how AI can defensively detect coordinated campaigns, identify influence networks, monitor executive personas, and provide early warning and substantially reduce risk.

As enterprise AI adoption accelerates, organizations must protect not only infrastructure and data but also the integrity of the information consumed by employees, executives, investors, customers, and AI systems. Digital trust should become a measurable element of cyber resilience.

FIVE RECOMMENDATIONS FOR CISOS

1. **Treat narrative attacks as enterprise cyber risk rather than solely a communications issue.**
2. **Integrate narrative intelligence into security operations and threat intelligence workflows.**
3. **Update incident response plans to address deepfakes, executive impersonation, synthetic media, and coordinated misinformation campaigns.**
4. **Extend AI governance programs to include narrative security and protection of digital trust.**
5. **Measure digital trust using meaningful metrics that complement traditional cybersecurity performance indicators.**

CONCLUSION

The modern CISO is ultimately responsible for helping the organization maintain trust in an increasingly AI-driven world. As offensive AI automates the creation and amplification of narrative attacks, defensive AI must become part of the security architecture.

Organizations that treat narrative intelligence security as an extension of cyber resilience—rather than an isolated communications function—will be substantially better positioned to protect their executives and company reputation, financial performance, operational resilience and stakeholder confidence. We believe narrative intelligence will become a standard capability of leading enterprise security programs during the next several years.

ABOUT TAG

Recognized by Fast Company, TAG Infosphere is a next-generation cybersecurity and artificial intelligence research and advisory firm that combines experienced analysts with an AI-powered research platform to deliver on-demand intelligence, executive education, and strategic guidance to enterprise teams, government agencies, investors, and technology providers.

Copyright © 2026 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.