Teneo®

From Fake News to Real Consequences: Disinformation's Growing Impact on Business

October 30, 2024

A well-known pharmaceutical company posts on X (formerly Twitter) that it will offer free insulin. A Department of Defense memo circulates among lawmakers questioning a corporate acquisition based on considerations from the Committee on Foreign Investment in the United States, or CFIUS. A communications leader for a cryptocurrency exchange platform reaches out to the community via Zoom with commentary on the industry. Meanwhile, a CFO deepfake successfully secures a $25M wire transfer from an unsuspecting employee. What do all these seemingly random examples have in common? They all happened and were all forms of disinformation attacks.

Disinformation, a longstanding weapon for discrediting and harming candidates in the political arena, has evolved from a tool used to disrupt elections and undermine public figures into a sophisticated instrument for attacking global businesses. Governments and political operatives have exploited false narratives to influence public opinion, using disinformation campaigns to undermine adversaries or stoke societal divisions. With the rise of powerful technologies, the scope of disinformation has expanded dramatically. What was once largely confined to the machinations of state actors and partisan political warfare has

entered the corporate realm, with malicious actors now targeting businesses for financial gain and reputational damage.

What can organizations do about it? This article addresses the current threat landscape and proactive best practices in disinformation detection, mitigation and response.

From Traditional to Social Media

Information fabrication, or "disinformation," is not a new concept. Every major world war has involved disinformation attacks through tactics such as word of mouth, pamphlets, radio, and later, television. Prior to social media, disinformation could make the rounds on traditional media channels but could be debunked through fact-checking or clarifying statements from the target of the attack.

Fast forward to the advent of social media. Society is increasingly dependent upon real-time, on-demand breaking news served up on smartphones in the palm of our hands. A 2022 Pew Study noted that roughly one-third of U.S. adults trust the news they see on social media, while 50% of 18- to 29-year-olds in the U.S. say they have some or a lot of trust in the information they read on social media.[1] These statistics are startling, with social media serving as a primary and priority source of news and information – where just about anyone can publish "news" content at any time.

Recent advances in AI have exacerbated the challenges with disinformation. AI tools available today enable the creation of hyper-realistic fake content, including deepfakes—audio, video and text simulations—that are virtually indistinguishable from authentic content. Deepfakes are increasingly disseminated via social media and other digital platforms to manipulate stakeholder trust, generate market volatility and tarnish corporate and executive reputations. The ease with which this content can be created and shared across platforms means that even small-scale threat actors can deploy large-scale disinformation campaigns with damaging consequences for businesses and their leaders.

Today, companies face disinformation threats that extend far beyond the occasional negative headlines or rumors. While organizations have been focused on building up their cybersecurity capabilities to address the rise in global data breaches, ransomware attacks and phishing scams, disinformation attacks are newer to the cyber-attack playbook. Corporate entities are now in the crosshairs of cybercriminals, hacktivists, hostile competitors, conspiracy theorists and professional trolls, who use fake news and forged content to manipulate public perception, erode trust and create financial harm. In the financial services sector, bad actors are using deepfake audio and video to trick employees into fraudulent transactions. Whether it is a falsified financial report, a fabricated scandal involving key executives, a doctored video of a product malfunction, or fake audio of a company official requesting a financial transaction, the consequences can be dire: stock price fluctuations, monetary loss, customer attrition

Corporate entities are now in the crosshairs of cybercriminals, hacktivists, hostile competitors, conspiracy theorists and professional trolls, who use fake news and forged content to manipulate public perception, erode trust and create financial harm.

[1] US adults trusting news from social media at record level | World Economic Forum

and regulatory scrutiny. Businesses that once viewed disinformation as a problem confined to the political realm must now recognize it as a direct and serious threat to their operations and bottom line.

Content Moderation and Regulation is Not Enough

In theory, content moderation on social media, coupled with relevant regulation to prevent the creation and spread of disinformation, should serve to help reduce its proliferation. However, content moderation faces challenges in execution, while regulation often lags behind the advances in the technology that facilitates the spread of falsehoods.

On the regulatory front, particularly in the U.S., there is no federal legislation, and most states are working on passing or have passed their own version of an AI-generated disinformation bill into law, creating challenges for businesses operating nationally or internationally as they seek a clear understanding of their legal rights and obligations.[2] The EU and UK have made additional federal strides but progress is by no means universal. There is significant momentum in 2024 to tackle disinformation globally, but lawmakers face challenges in instituting legislation today that may not be fit for purpose tomorrow as AI tools and technology advance.

Content moderation also has its challenges and complexities, given the volume of content subject to moderation, rapidly evolving disinformation tactics, difficulty in determining context in social media posts, concerns over free speech infringements and the ease with which disinformation spreads. For now, while social media platforms and regulators chase technological developments, organizations and executive leadership teams will have to take matters into their own hands to protect corporate and brand reputation, as well as themselves.

[2] US state-by-state AI legislation snapshot | BCLP - Bryan Cave Leighton Paisner

The Fog of (Disinformation) War: The Role of Corporate Branding, Stakeholder Equity and Communications

No brand is immune to disinformation, whether a global household name or one known primarily within its industry. Notable disinformation campaigns and deepfake attacks have targeted industries including pharmaceutical, cryptocurrency, financial services and entertainment. While some companies recovered quickly with limited impact, others suffered significant media attention and financial loss. Breaking through disinformation requires trust in a company's brand and a clear understanding of what the company represents to its most important stakeholders.

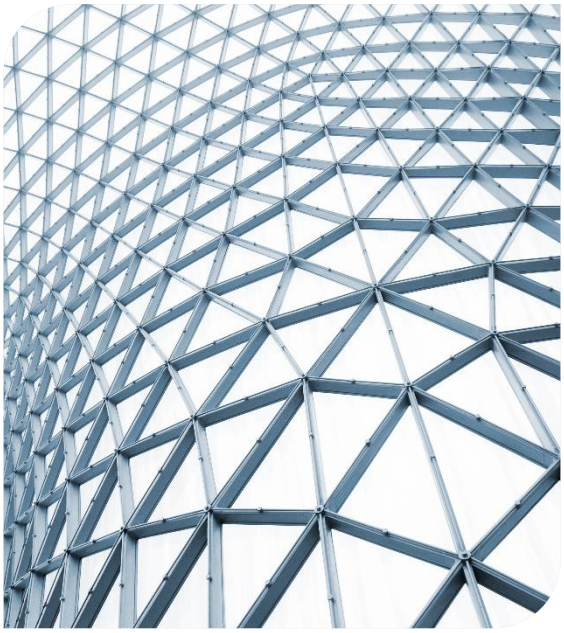
As with other types of attacks, preparation is key to being able to extinguish or blunt a disinformation attack quickly. Prepared organizations establish reputational equity through a clearly expressed narrative that defines the business' differentiators, mission, vision, values and reason for being. Equally important, businesses must establish a disinformation response protocol through crisis planning, understanding that fighting disinformation may require a broader set of capabilities than traditional crisis management.

Teneo's Disinformation Detection, Mitigation and Response Offering

We predict that, much like a ransomware attack or other targeted cybersecurity incidents, disinformation attacks are now a matter of "not if, but when." Similar to traditional cyberattack defense, companies do not have the luxury of deprioritizing disinformation detection and response, especially when tools and capabilities to cause harm are outpacing traditional mitigation tactics.

Disinformation attacks happen unexpectedly and escalate quickly, and a lack of action (or the wrong actions) can cause further damage. The complexity of the first hours and days of a disinformation attack requires organizations to determine the following quickly:

- How best to remove or flag false content
- The true reach of disinformation across social and digital spaces
- The core source of the disinformation and the motivation(s) behind the attack
- Perception by various stakeholder groups and real-time evolving sentiment
- Potential market and financial impacts
- The need for public statements and internal communications
- How best to construct an effective counternarrative strategy
- Potential safety and security implications for key executives and other targets



Our experts deliver a cross-disciplinary, holistic program designed to proactively safeguard corporate reputation, brand well-being and executive positioning. We provide both the tools and the advisory services to prepare organizations to detect, mitigate and respond to disinformation threats.

Our cross-functional team of subject-matter experts leverages proprietary technology and assessment capabilities to provide clients with unparalleled services and solutions to prepare for and respond to disinformation attacks.

Our social media listening, digital monitoring and threat intelligence tools can identify early warning indicators of false narratives and flag or remove inaccurate content. If a narrative becomes a full-blown disinformation campaign, our team will assess the impact and work with clients to design and manage the operational and communications response.

How We Engage with Our Clients

Disinformation Preparedness

- **Corporate Narrative Development**: Creation of a strong foundation for your business to build understanding among key stakeholders and develop proactive internal and external communications campaigns.
- **Anticipating and Surfacing False Narratives**: Identification of emerging false narratives targeting the brand and/or executives using Teneo's risk intelligence and digital tools, while removing or flagging toxic and harmful content.
- **Building Crisis Response Structures:** Review and assessment of the company's existing crisis management capabilities to ensure they are fit for purpose for disinformation and deepfakes.
- **Disinformation Crisis Simulations:** Implementation of immersive and sophisticated executive crisis simulation exercises to evaluate the ability to effectively respond to and manage a disinformation attack.

Disinformation Crisis Response

- **Crisis Team for Disinformation Attacks:** Immediate mobilization of Teneo's Digital Protection team to support organizations and leaders through all facets of a disinformation attack.
- **Disinformation Source(s) Investigation:** Investigation of the disinformation source to better understand their identity, reach, impact and motivations.
- **Comprehensive Impact Assessment**: Cross-domain analysis of the incident's impact on the market/financials, stakeholder perception, social media traction, emerging narratives and potential security implications for employees or executives.
- **Crisis Communications Strategy***:* Development of immediate crisis communications support and recommendations, including stress-testing messaging and responses across various stakeholder groups.

Post-Incident Resilience

- **Proactive Social Media Monitoring and Emerging Issue Escalation:** Definition and implementation of an ongoing social media monitoring program to increase intelligence and awareness post-incident, surface new false narratives and support with content flagging or removal.
- **Strategic Communications:** Development and execution of long-term strategic communications plans based on incident severity and impact.
- **Training and Preparedness:** Leveraging lessons learned from the attack to build and deliver training and enhance preparedness capabilities.

Key Contacts

For more information about Teneo's Disinformation Detection & Response offering, please contact:

Courtney Adante
President, Security Risk Advisory
courtney.adante@teneo.com

Andrew Lee
Senior Managing Director and Head of Teneo Digital
andrew.lee@teneo.com

Bethany Sherman
Senior Managing Director
bethany.sherman@teneo.com

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com