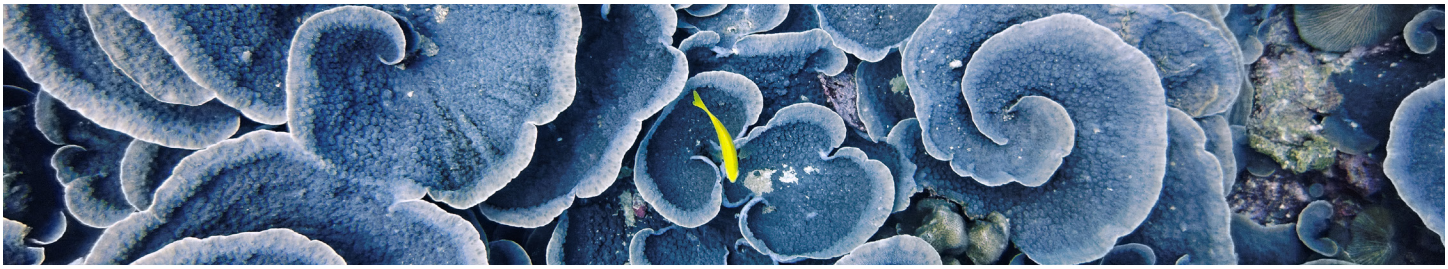

The threat misinformation and disinformation pose to business

Disinformation and misinformation are emerging as significant cyber threats to businesses worldwide. Learn about their potential risks and how best to combat them.

Key takeaways

- Disinformation is verifiably false information created and disseminated with intent to deceive, whereas misinformation is false information shared without malicious motive.
- Risks to businesses targeted by mis/disinformation include financial losses; erosion of market confidence and customer, client and employee trust; and slowdowns in rolling out new technology or products.
- The best defense is to develop a strategy for strengthening company reputation and addressing falsehoods as part of the overall response plan.

The spread of false information is not a new threat. Disinformation in the form of fake news stories, hoaxes and propaganda has been used to engender public cynicism and distrust since the invention of the printing press. But false narratives could only spread as fast as they could be printed and distributed — until now.

With the ubiquity of the internet and popularity of social media, disinformation, and its close relative misinformation, can now be spread faster than a mouse click — an advance with potentially dramatic consequences for businesses. To protect against such threats, organizations must understand not only the risks they pose to business objectives, but also how and why disinformation and misinformation are able to spread and succeed. Only then can organizations form long-term strategies to defuse false information and halt potential damage.

While the terms are often used interchangeably, misinformation and disinformation are two separate threats. Disinformation is verifiably false and/or manipulated information that is created and disseminated with the intent to deceive. Modern examples of disinformation include sensationalist stories on phony websites, deliberately dishonest memes posted to social media and fake videos generated by artificial intelligence called deepfakes (see *How to protect your business from deepfakes*).

In contrast, misinformation is false information shared without malicious motive. Examples of misinformation include erroneous emails shared by someone who believes the information is real or unverifiable rumors circulating on a forum thread. Both disinformation and misinformation spread falsehoods — their difference lies in intent. Either way, thanks to the proliferation of technology, the velocity, reach and rate of mis/disinformation have increased exponentially.

Tools of the mis/disinformation trade

Mis/disinformation differ from typical cyber threats such as malware in two ways: who is behind the threat, and how it is made and disseminated. While some who develop disinformation are profiteers looking for financial gain, many times they are nation states, extremists, provocateurs, disgruntled former employees or even business competitors. Criminals can now produce and propagate disinformation with relative ease because there's no need to physically, or even virtually, infiltrate a country or business network. Inauthentic content can be crafted in blogs, emails and social media posts.

Social media and memes

Memes are a popular format for disinformation: They're fast and easy to make, appeal to a wide range of age groups and have high viral potential.[1] False stories and memes proliferate on social media, where a particularly controversial post can generate optimum engagement (usually in the form of heated debate), build a larger following and subsequently trigger viral spread to multiple other media channels. Notably, memes posted to social media allow threat actors to operate in a gray area and damage a business' reputation without exposing themselves to the fallout of any conflict.

Forgeries

Disinformation can also take the form of forgeries, which typically feature fake letterheads, copied and pasted signatures and maliciously edited emails. To make forgeries seem more credible, threat actors claim they are from a hack, theft or other document interception — "leaked" materials. And they may include legitimate content to lend authenticity to their messaging.

Synthetic media

Because people are naturally more likely to believe what they see, synthetic media such as manipulated photos and audio and video deepfakes are especially convincing and dangerously effective. Without sophisticated software, it can be difficult to determine the authenticity of these forms of disinformation.

Proxy websites

Another way cyber criminals develop disinformation is through proxy or fake websites. Proxy websites are fronts designed to disguise the source of content or use that content to drive pageviews. These sites often crop up after newsworthy events, playing on the public desire for more information. The only way to discriminate between a legitimate website and a proxy is to scrutinize the URL for misspellings or cross-check the site's information with verifiable sources.

Content farms

To distribute their deceptive content, cyber criminals use a number of platforms and technology services. Content farms, also known as content mills, generate large quantities of low-quality web content designed around search engine standards to display them higher in search results — a practice known as search engine optimization (SEO). While SEO is a legitimate marketing practice, churning out false content to target popular searches and drive advertising revenue is not. Disinformation and misinformation spread quickly through content farms, as their goal is to attract a high volume of web traffic at all costs.

Botnets

Botnets are often used to amplify disinformation engagement on proxy websites and social media. A botnet, short for robot network, is a network of computers (bots) infected by malware and leveraged by a single person, who can command each bot to simultaneously carry out a coordinated action. Bots can generate fake social media and commenter profiles, making it difficult for the average user to tell the difference between bot and human. The sheer size of a botnet — some with millions of bots — enables cyber criminals to manipulate public sentiment on a massive scale.

"Criminals can now produce and propagate disinformation with relative ease because there's no need to physically, or even virtually, infiltrate a country or business network."

Disinformation-as-a-service

Finally, disinformation-as-a-service (DaaS) models are now popping up to assist in creating faux social media identities and using them to either boost a reputation through fake reviews, testimonials and news stories, or to tarnish one using the same methods. DaaS can target both individuals and organizations, and it's often fairly inexpensive, ranging from under $100 to $100,000-plus. DaaS agents have emerged in many countries, and they routinely advertise to the private sector.

[1] Benjamin Barack, Poynter, "How memes are used to spread misinformation," March 2022.

The risks for companies

While mis/disinformation are best known for their impacts on global politics and public health discourse, these dual threats are also being used to target businesses large and small, as well as individual employees. Certain characteristics may make an organization or individual more likely to become a victim of disinformation.

- Visibility factors, such as name recognition, profitability, company size and public controversy
- A significant social media presence for the business or its executives
- Public stances on controversial political, social or environmental issues
- A merger, public transaction, major deal, rebranding or reorganizing effort
- A new product or service in high demand

Unfortunately, any business can become a target of disinformation.

- In 2017, a small Indian restaurant in London was falsely accused of serving human meat on Facebook — the family business subsequently saw its revenue cut in half.[2]
- In 2020, a Reddit post accused a major furniture retailer of being part of a child-trafficking ring.[3] The next day, posts affirming the theory were found widely circulating on social media, and accusations were still floating on YouTube a year later.
- In 2018, a forged U.S. Department of Defense memo stated that a semiconductor giant's planned acquisition of another tech company raised national security concerns, causing stocks of both companies to fall and merger talks to temporarily stall.[4]

Misinformation can also pose a risk to businesses. On a Saturday morning in 2019, a rumor began on WhatsApp that a U.K.-based bank was facing financial difficulties and might shut down. By 4:00 p.m., there were lines of anxious customers outside several branches looking to close out their accounts or empty safe deposit boxes. Although the rumor wasn't true, it came on the heels of a highly publicized accounting error by the organization as well as a poorly performing stock[5] — rendering the rumor more believable. When markets opened on Monday, the bank's share price tumbled 9%.[6]

The risks of mis/disinformation to organizations are threefold: reputational loss, financial loss and disruption of business objectives. All are intricately connected, with reputational loss potentially leading to financial trouble, and financial trouble potentially leading to delays in taking on or completing new projects. Underestimating the fundamental risks of mis/disinformation could have dire consequences. That's why it's crucial to examine how these threats could affect your company before formulating a defense strategy.

[2] Matthew Ferraro and Jason Chipman, *The Washington Post*, "Fake news threatens our businesses, not just our politics," February 2019.
[3] Marianna Spring, BBC News, "Wayfair: The False Conspiracy about a Furniture Firm and Child Trafficking," July 2020.
[4] Reuters, "Pentagon says memo asking for Broadcom-CA deal review is likely fake," October 2018.
[5] Jim Edwards, Insider, "A false rumor on WhatsApp started a run on a London bank," May 2019.
[6] Amit Katwala, *Wired*, "The Metro Bank hoax shows the immense power of fake news on WhatsApp," May 2019.

Reputational loss

The effects of reputational loss can register with customers, investors and partners to varying degrees, with potential for calamitous repercussions. The aftermath may also extend to shareholders, impacting investor confidence and causing stock values to plummet. If a mis/disinformation threat is extensive enough, it could also spill over to employee faith in the organization, which would not only affect productivity, but also recruiting, staff morale and retention.

Financial loss

Deterioration of trust in your brand due to mis/disinformation often has a ripple effect on your bottom line, resulting in lost profits and future sales, as well as reductions in share prices. Delays in rolling out new products could further impact customer satisfaction, provoking an exodus of loyal clients to competitors or a massive contraction of earnings, leading to an endless cycle of loss.

Disruption of business goals

If mis/disinformation results in lost profits, product roadmaps, professional development initiatives and other business goals will likely experience setbacks, if not suspensions or cancellations. Budget cuts to IT and security could stall important mitigations, allowing for cyber criminals to capitalize on vulnerabilities and compromise business networks. In addition, new technologies may not be implemented in a timely way, leading to a competitive disadvantage against other companies or countries. For example, online stories between late 2018 and 2020 claimed that 5G wireless was responsible for the death of hundreds of birds,[7] would give people diabetes and was being used to spread COVID-19, resulting in the destruction of several cell phone towers and equipment boxes in Britain.[8]

"The risks of mis/disinformation to organizations are threefold: reputational loss, financial loss and disruption of business objectives."

Proactive defense against misinformation and disinformation

Protecting against mis/disinformation is tricky business. A 2018 study by researchers at MIT found that false rumors spread more rapidly and more widely than facts, with falsehoods 70% more likely to be retweeted on Twitter, reaching their first 1,500 people six times faster than the truth.[9] Once a negative rumor about an organization begins circulating online, it's much harder to counter — even with the truth.

Therefore, the best defense for potential targets of mis/disinformation is to go on the offensive. Here are several ways companies can proactively protect against falsehoods:

- Get buy-in from the top. First, convince an executive, such as a CEO, CISO or IT director, that defending against disinformation is important. Leadership is needed to commit the resources necessary to combat mis/disinformation. Otherwise, stakeholders may not be compelled, or even feel they have license, to act.
- Assign ownership for developing prevention, mitigation and response policies. Having a person or team with direct responsibility will ensure that any strategies formed will yield tangible, actionable results.
- Develop a communication plan and templates that address media inquiries, as well as employee and vendor questions. This will allow your organization to quickly defend its viewpoint. Depending on your company size and perceived risk, it may be logical to have a communications firm on retainer.
- Develop programs for establishing and maintaining company reputation internally and externally. Extend reputational efforts outside the proverbial company walls in multiple communications formats, from thought leadership in the press to product-agnostic blogs on your website. Cultivating a trusted reputation will blunt damage from mis/disinformation and builds long-term trust in your brand.

[7] Alex Kasprak, Snopes, "Did a 5G Cellular Network Test Cause Hundreds of Birds to Die?" September 2019.
[8] Frank Langfitt, NPR, "5G Conspiracy Theories Trigger Attacks On Cellphone Towers," April 2020.
[9] MIT Sloan School of Management," Study: False news spreads faster than the truth," March 2018.

Defense against internal misinformation and disinformation

To best protect against mis/disinformation, it's equally important to examine your internal company culture and the way in which information is shared among employees. Troubleshoot for lack of transparency or rumors about people, departments and the overall health of the organization. Establish policies and educational programming around misinformation, remembering the potential for backlash against mitigations that could be perceived as exerting too much control over employees. Your policies must match your organization's culture to be effective.

Here are some protocols that help limit the spread of mis/disinformation from staff:

- Draft simple, clear rules in the company handbook about what is acceptable to discuss internally vs. what is allowed or prohibited on social media and elsewhere online. Many organizations restrict employees from posting proprietary data or other business content unless using approved messaging.
- Communicate your rules effectively. Outline all guidance on social media policy during the onboarding process and store it in a central company repository.
- If you do allow employees to speak freely about the company on social media, require that they include disclaimers stating all opinions are their own. This may offer additional legal protection if employees post derogatory or inflammatory comments.
- For employees having trouble following policy, educational programs on digital literacy could be useful. Digital literacy programs help users discern best internet practices and indicators of truth, including how to tell if online content is accurate or where to find reputable sources. These programs could establish your workforce as exceptional digital citizens, accurately informed and impervious to disinformation, which may also improve company reputation.

Once you've determined a few mis/disinformation parameters for staff, you should contemplate how to enforce them. What are the consequences of breaking the rules? You can't suspend your employees' personal social media accounts, but you might be able to restrict social media use while on a work computer or at the office. Again, company culture can guide organizations in what would be considered acceptable by staff.

Detecting misinformation and disinformation

Mis/disinformation are emerging threat vectors for businesses, so new technologies are still being developed to protect against them. However, there are several best practices to help companies detect false information about their brand or employees online.

- Consider partnering with third-party consultants who specialize in reviewing social media for disinformation keywords and unsubstantiated mentions of your company name.
- Evaluate automation tools that use AI and machine learning to scan social media platforms for falsified information, or companies that evaluate unstructured data, such as video and audio manipulations.
- Businesses should also monitor their own online platforms by setting search alerts for relevant terms and high-profile employees. Understand what people are saying about your corporation, organization, services and staff. Is the language they use positive, neutral, negative or nonfactual?

- Set up verified social media profiles in all platforms, especially newer ones, to protect against spoofing — even if you don't plan on posting.

Keep in mind, detection tools can only go so far. They may flag a suspicious element, but you still need to verify whether it's false. And although these companies and tools may be able to scan social media posts for inauthentic content, it's harder on private channels like instant messaging apps.

Best practices for mis/disinformation response

While there may be limited solutions for preventing or mitigating mis/disinformation, businesses can focus on response techniques. Have a plan so that if an incident does happen, your company can spring into action before rumors spread too far. Use the same channels you developed for reputational content to succinctly counter falsehoods: You don't want to escalate into snippy online battles.

To counter the ambiguous threat of mis/disinformation, organizations should move beyond conventional thinking and consider creative response solutions instead. These might include:

- Conducting tabletop exercises for mis/disinformation events; establishing drills for falsehoods that impact customer, client and employee trust
- Assigning roles and distributing communication trees for escalation if a mis/disinformation incident occurs, including weekend and emergency contacts
- Drafting templates for press releases countering potentially false claims with updated public facts
- Developing relationships with journalists, influencers or other online personas who could be quickly reached to help defuse mis/disinformation

Misinformation and disinformation are not new, but their rapid uptake online and on social media have rendered them far more dangerous than in the past. As mis/disinformation threats against businesses increase, it's important to remember how difficult they can be to untangle — and how detrimental they can be to an organization's reputation, operations and bottom line. Ultimately, the best defense is to be in control of the narrative from the start. ■

For use in external marketing and communications materials when the content of the material discusses both products and services offered through the bank and broker/dealer affiliates.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.
Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value

BANK OF AMERICA