protiviti®
Face the Future with Confidence

Are Bad Actors Looking to Cause Corporate Havoc With Disinformation? Bogus Whistle-blower Complaints Are Making the Rounds

30 July
2021

"Misinformation" and "disinformation" have long been mainstays in the political arena, the climate change debate and even in the public discourse over COVID-19 vaccines. Misinformation represents information that is wrong, a challenge every business must deal with from time to time, whether in the press, analyst communications, social media, discussions at government levels, or other venues. Disinformation is also information that not only is wrong, but is intentionally wrong. Often relatively easy to launch and hard to defend, disinformation may become a common phenomenon in the business environment in a wide variety of forums and perpetrated by many types of bad actors over the forthcoming decade, including nation states, political extremists, extortionists or disgruntled employees.

Disinformation campaigns may target specific companies or even whole industries. No organisation can expect immunity. The nature of these campaigns requires a broader discussion. However, this Flash Report specifically is intended to alert companies to a specific disinformation issue as it involves the creation and spreading of false messages. In an already challenging IT and information security environment in which cyber breaches, ransomware attacks, pervasive phishing scams and numerous other threats continue to vex organisations, there now is a growing trend of disinformation making the rounds through hoax whistle-blower complaints.

A valued channel for feedback is being abused

With some being confidential and others being anonymous as well, hotlines are an essential and valued source of input, feedback and intel on a wide variety of topics. These channels can help expose dysfunctional issues, toxicity in the workplace, irresponsible business behaviour and even illegal activity.

Unfortunately, as reported in a number of legal sources, including TheCorporateCounsel.net and the Association of Corporate Counsel, a growing number of companies are receiving anonymous whistle-blower complaints that are proving to be hoaxes. The motivation for these ruses currently is unclear. They were uncovered based, in part, on the fact that

multiple organisations had received complaints with nearly identical wording. Outside law firms that were consulted identified a pattern in the similar wording within these complaints and raised a red flag.

What is particularly challenging with these bogus complaints is that they are well-written and convincing. Frequently, phishing emails and more obvious scams contain a few tell-tale signs, including poor spelling and grammar. However, these complaints are constructed in a clever manner and could easily spur an organisation into a quandary of indecisiveness or even a full-scale investigation that wastes time and resources.

Bottom line, amid a myriad of other cyber and information security concerns, organisations must also face the risk of disinformation in their complaint reporting channels and the resulting challenges it can create.

Steps organisations can take

While some may suggest doing away with anonymous whistle-blower reporting and requiring individuals filing complaints to identify themselves, current regulations prohibit that approach for many organisations. As an example, in the United States, under requirements in the Securities and Exchange Act of 1934 and Section 301 of the Sarbanes-Oxley Act of 2002, public reporting organisations must establish procedures for handling complaints regarding accounting practices. Specifically, audit committees are required to establish procedures for:

1. The receipt, retention, and treatment of complaints received by the listed issuer regarding accounting, internal accounting controls, or auditing matters; and
2. The confidential, anonymous submission by employees of the listed issuer of concerns regarding questionable accounting or auditing matters.

Other organisations, while not required legally to establish such procedures, frequently incorporate these practices into their hotline network, particularly to provide the opportunity for individuals to submit complaints anonymously.

Thus, organisations need to implement other steps to ensure they are able to manage and mitigate the potential new risk of disinformation within their complaint reporting process. These steps should include the following:

1. Review any anonymous complaint thoughtfully and involve the right team to evaluate the complaint, including general counsel and the audit committee.
2. Attempt to gather more information from the anonymous filer through the hotline service, if possible. In some cases, the hoax has been a one-time complaint and no responses are provided after multiple follow-up inquiries asking for any additional details to aid in an investigation.
3. If the complaint appears to have credibility and involves a serious matter, consult with outside counsel to ascertain whether it fits a pattern of similar complaints received by other companies.
4. If applicable, check with your hotline service provider regarding irregularities and issues they may be experiencing that are systemic or could be obvious hoaxes.
5. Monitor legal publications, such as the ones referenced above, and check with external auditors and internal audit service providers regarding market trends and experiences with other companies.
6. Depending on the results of the above steps, formulate an investigation plan and execute that plan within a reasonable time period.

Those executives responsible for the company's hotline network should be mindful of this emerging trend. The above steps can avoid time-consuming and expensive investigations into false allegations of wrongdoing. It is important that a cross-functional approach to these matters be taken to avoid legal, cybersecurity, internal audit or other functions that are operating in silos wasting resources turning over stones.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®