

A New Approach for Protecting Confidential Information During an Employee Activist Campaign

BY BRADFORD K. NEWMAN

October 23, 2024

Employee activism can be defined as actions employees take to change corporate decision-making by publicly applying pressure to the brand, board, shareholders, and customers. Once regarded as a vagary of a few socially conscious tech workers, employee activism has spread across industries in the form of “takeovers” of executive working spaces, public protests, social media campaigns, and public dissemination of confidential corporate information. With a crop of fresh college graduates who view activism as part of their identity entering the workplace, ongoing strife in the Middle East, and the November Presidential election on the horizon, employee activism is anticipated to increase. Based on the failure of corporations to stop the leaking of confidential business data amid these campaigns, a new approach is needed.

In 1970, economist Milton Friedman originated the concept of “Shareholder Primacy.” According to this, the sole purpose of a corporation is to maximize profits and value, consistent with law and ethical customs. The inherent logic is that only people, not enterprises, have social responsibility.

A half century later, perceptions radically shifted. A 2022 Bain & Company survey of business leaders revealed that only 15% believed business’ primary



Credit: Song_about_summerAdobe Stock

purpose should be to “maximize shareholder value,” while an overwhelming 39% prioritized balancing the needs of “all” stakeholders. Companies have responded by pursuing ESG initiatives, taking stands on social issues, and releasing Corporate Social Responsibility reports.

Employees share this viewpoint. The Edelman 2022 Trust Barometer Survey of global employees across 25 countries found when considering a job, 60% expect the CEO to speak publicly about social and political issues they care about. A recent Bentley-Gallup Business in Society Report similarly found that in the United States, younger workers

want businesses to take a stand on issues including climate change, economic inequality, workforce reskilling, access to healthcare, and social injustice.

Employees who find their beliefs in conflict with their employer's feel justified initiating and participating in workplace activist campaigns. Demands for internal culture reforms, the cessation of business relationships with certain political actors, changes in products, and ESG criticisms are common.

One key tool utilized by today's activists is the unauthorized disclosure of sensitive company data. This publicly bolsters demands by acting as "evidence" to activists' claims. Traditional management response tactics have proven ineffective in preventing data theft and leakage.

In the past few years, tech giants have been especially susceptible to the public disclosure of confidential internal documents by activists. Despite facing a high level of risk, tech companies have been the most outwardly vocal about following the traditional yet largely ineffective HR approach of engagement, but still face criticisms from all parts of the political and social justice spectrums.

The Current HR Approach

Academic and industry scholarship on employee activist campaigns reveals a uniform approach with origins in 1970-style management tactics used to oppose unionization efforts. This wisdom counsels companies to listen to issues employees raise, accommodate demands wherever possible, and empower employees to make changes. There is a simple reason traditional HR principles have today proven ineffective. Even in the adversarial environment between union organizer and employer, both sides remained motivated by a shared end-goal: a continued employment relationship between the parties, albeit according to the terms of a newly negotiated collective bargaining agreement.

Unlike union organizers, modern activists often seek to change the nature of a company and how it

conducts business — often in ways that are adverse to the company's core interests. In this scenario, traditional HR approaches fall flat as the company cannot change its business model to fit activist demands. Leaking confidential data is becoming a routine and damaging tactic that pulls companies "off-mission."

A New "Data Protection"-Focused Approach

When an activist campaign emerges, protecting confidential information must be of paramount concern. Below are the contours of a new data-protection approach responding to activist campaigns. Based on a cross-disciplinary process that involves Information Security, Legal, Communications, Site Security, and Human Resources, it is designed to empower companies to lawfully protect their most valuable confidential information while updating their activist campaign response.

1. Set A Business-Focused Corporate Policy

The goal is to establish a corporate culture that seeks a moderate marriage of Shareholder Primacy with the larger notion of Corporate Purpose. Companies must be moral and recognize prevailing attitudes toward employers held by today's younger employee base, but not devote to social causes that don't advance their business purpose.

The C-suite should communicate, through a formal Social Issues Policy, that corporate focus is on taking actions that benefit its customers and strengthens its products, while placing an emphasis on doing so in a way that furthers reasonable efforts to improve communities, the environment, and society. The policy should acknowledge employees will hold differing personal beliefs about social and political issues, but the workplace is not where business decisions will be made based on employees' personal viewpoints.

2. Forensic Review of the Activist's Past Data Access and Handling

Immediately upon learning of a campaign, companies should conduct a full forensic review of

the activists' computer usage going back at least 90 days to search for unauthorized access to and/or sharing and exfiltration of confidential company data. This process should be designed to determine whether the activist has accessed confidential information for which there is no business purpose and/or unlawfully shared it with coworkers or outsiders. It is important to note that a server-side only review of computer usage is not sufficient. A full forensic image of the activist's company computer and work cell phone should immediately take place.

3. Real-Time Computer Usage Monitoring For Exfiltration. The sole goal is to prevent the activists and their agents from unlawfully accessing and leaking confidential data. Where lawful, the company should consider ongoing real-time electronic monitoring.

4. When A Leak Occurs, Employ Specific Measures to Prove The Activist Is The Culprit. It is common for media to obtain and publish confidential information directly related to an ongoing campaign. Despite sophisticated tools, there may be no way to determine if the data was downloaded and disseminated by the activist. This is especially true where the data might have been accessed by the activist weeks or months before the campaign started.

In this scenario, companies should consider employing the following methodology to identify the leaker:

1. Create an internal document that purports to contain sensitive information related to the activist campaign.
2. Before disseminating the document to the activists, insert different key information (dates, figures, key facts) into each version.
3. Prior to dissemination, separately assign each unique version to a different suspected activist.

4. Disseminate the documents.

5. Depending on which unique version of information is subsequently leaked, it is easier to identify the leaker.

6. Terminate the leaker(s) for IP policy violations.

The corporation has an obligation to protect itself from further leaks, even as activists try to avoid detection.

5. Comms Strategy. It is commonplace for employee activists to claim the company is retaliating against them. Once picked up by media channels, the allegation can cause reputational damage. The company should consider publicizing in a factual manner that there was a strong evidentiary basis to terminate the activist when possible.

Conclusion

Modern employee activists employ tactics to gain attention and seek credibility, often including the theft and dissemination of confidential corporate material. The traditional Human Resource response fails to prevent data theft and limit reputational and monetary damage to the company and its stakeholders. Companies facing these campaigns should employ a new data-protection approach.

***Bradford Newman** is Chair of Baker McKenzie's North America Trade Secrets Practice. According to Chambers USA, he is a «recognized authority on trade secrets cases» who «is valued for his tenacious, intelligent and thoughtful approach to trade secrets matters.» Bradford regularly serves as lead trial counsel in cases with potential eight and nine-figure liability, and has successfully litigated a broad spectrum of trade secrets cases in state and federal courts throughout the country. He routinely advises and represents the world's leading technology, health care, and financial services companies in connection with their most significant matters.*