carahsoft.

RANE
Risk Assistance Network + Exchange

¢KŜ /ƻyǾŜǋƎŜyŎŜ ƻŦ tKèăǿŎl-f l-yŘ /èōŜǋ !ŎúǿǾǿăY !Ǝl-ǿyăú !L l-yŘ !ŁπǋŜfl-úŜŘ Łyŧǋl-ăúǋdzŎúdzǋŜ

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies₿

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with w!b9, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/w!b9ǋŜăƻdzǋŎŜă

Join Events & Webinars:
carah.io/w!b9ŜǾŜyúă

Discover Technology Solutions:
carah.io/w!b9ăƻfdzúǿƻyă

Learn About /ƻYYŜǋŎǿl-f:
carah.io/w!b9ŏƻYYŜǋŎǿl-f

Connect With Our Team:
w!b9@carahsoft.com
тлопутмпурпу

E4C | GETTY IMAGES

The Convergence of Physical and Cyber Activism Against AI and AI-related Infrastructure

As AI usage proliferates globally, governments and individuals alike have largely fallen into two camps: pro-innovation and pro-safety. In the United States, the Trump administration has prioritized rapid development and minimal regulation to maintain a competitive edge, particularly regarding its rivalry with China.

This dovetails with efforts from large technology firms to accelerate global AI adoption, promoting its economic potential and embedding it across industries to reinforce expectations that AI will be a transformative, economy-wide shift.

Meanwhile, some lawmakers, like those in the European Union, fearing potential harms from the technology and widespread economic displacement, have taken a more precautionary approach, emphasizing safety, ethics and regulatory guardrails.

This divergence is unfolding against a backdrop of broader geopolitical instability and economic uncertainty, shaping how the public perceives the rise of AI. While governments and corporations often emphasize AI's potential to catalyze innovation and growth, public sentiment is more mixed and, in many cases, skeptical. This is especially true as experts have predicted that the AI revolution will upend nearly every industry, creating a phenomenon of growing economic and societal uncertainty among the general public.

Concerns around job displacement, bias, surveillance and loss of control have tempered public enthusiasm, contributing to a fragmented landscape of trust. Indicating these attitudes, a March 2026 NBC News survey of registered voters found that 46% of respondents actively held negative feelings towards AI, with only 26% viewing the technology favorably and 27% neutrally.

AI backlash could emerge from people across the ideological spectrum, ranging from environmental radicals on the left to neo-Nazi accelerationists on the right."

As competing perspectives of top-down optimism and bottom-up concern continue to collide, they create a more complex risk environment for organizations navigating AI adoption. To help us understand the risks of these two camps converging, we spoke to Sam Lichtenstein, Director of Analysis at **RANE**, and Isaia Galace, Lead Global Security Analyst at **RANE**.

Who Will Be Involved?

The AI backlash movement will draw a wide array of actors, representing an issue that overlaps with numerous pre-existing social movements and ideological followings. Lichtenstein tells us that "AI backlash could emerge from people across the ideological spectrum, ranging from environmental radicals on the left to neo-Nazi accelerationists on the right."

This means that extremist organizations and individuals across the ideological spectrum could come together on certain issues pertaining to AI. Lichtenstein adds that because of this, "There are a huge variety of previous movements and groups that could provide inspiration. These include: neo-Luddites/antitechnology radicals, eco-extremists, antiglobalization activists and anticapitalist groups… because grievances over AI are so wide, there are a huge variety of precedents that threat actors could draw on."

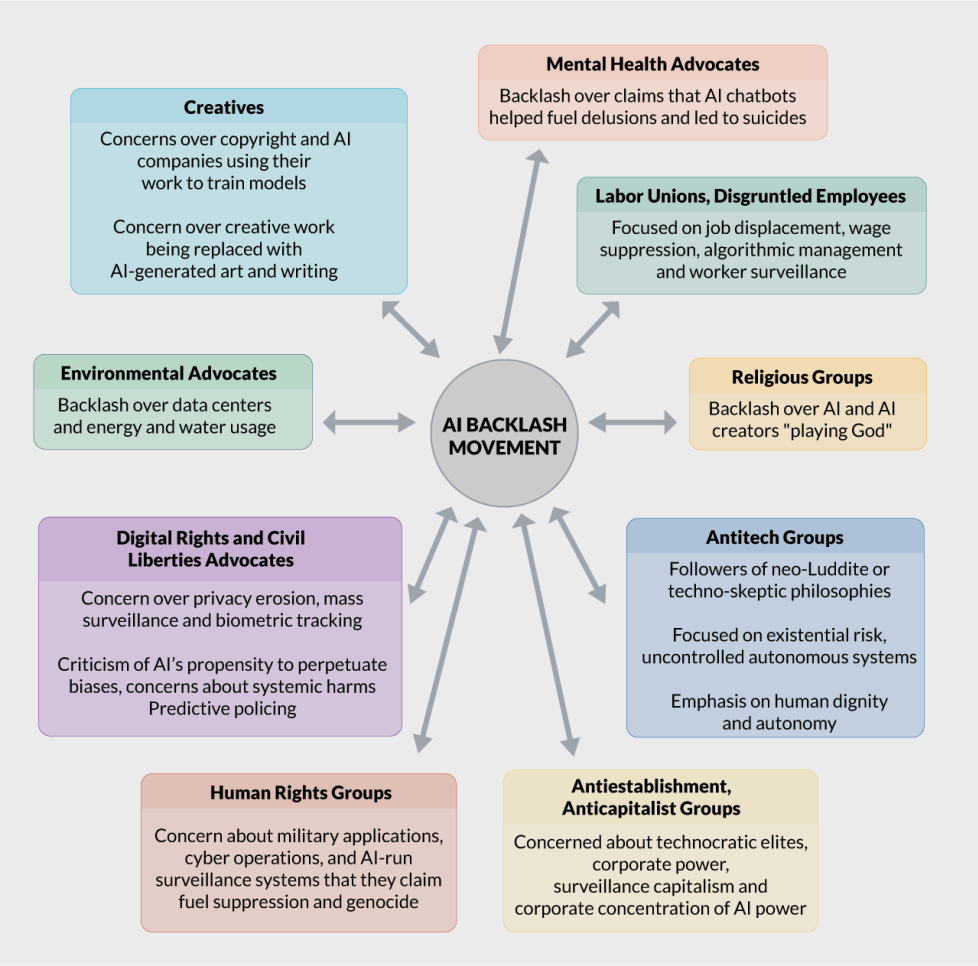
Regardless, Lichtenstein reminds us, "The biggest violent risks may not be organized groups or even loose movements, but instead lone actors and small cells acting on their own." This is especially true given the role that economic grievances will play in AI backlash, from job-specific impacts to general economic disruption and issues like rising energy prices, meaning that some issues do not fall under any one particular camp.

While both organized movements and lone actors may pursue action to address their particular grievances with AI, most are likely to be driven by a defined ideological motivation. Among the

range of motives, the primary ideological drivers can be grouped into the following categories, which are most likely to shape activism against AI:

Actors Involved in the AI-Backlash Movement

AI-backlash will draw in a wide range of actors and social movements, with various groups progressing both their own protests and collaborating with other groups in their efforts.



Source: RANE Analysis

Environmental Advocates

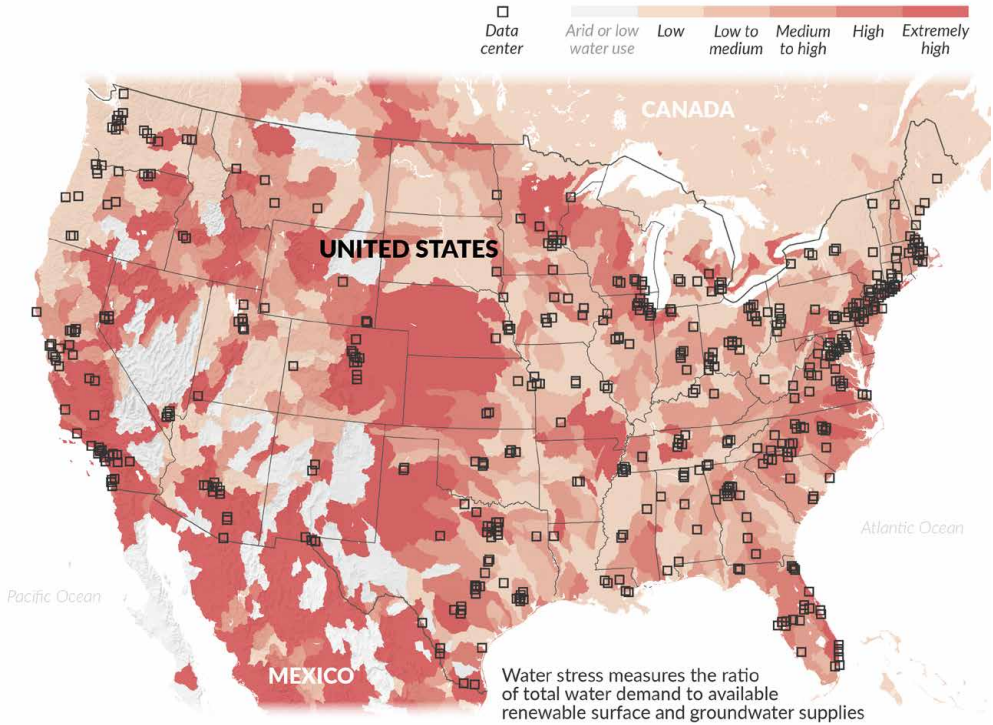
One of the most widely talked about concerns about AI has centered on energy consumption and the construction of water-intensive data centers, which can strain local infrastructure and cause harm to the surrounding environment. Because environmental movements have historically carried out wide-scale organized protests, site blockades and at times more aggressive action, like targeting infrastructure such as pipelines, mines and power facilities, this movement is more likely to prompt similar action against AI usage and infrastructure. Data centers, chip manufacturing plants, offices of AI companies and organizations implementing AI on a large scale, especially in Silicon Valley, are potential focal points.

One left-wing extremist group that may seek to target data centers or other infrastructure powering AI is the German-based Vulkangruppe, or Volcano Group. The group has carried out several high-profile attacks on critical infrastructure, including one against one of Berlin's largest gas-fired power plants in January that resulted in a blackout affecting more than 45,000 households and 2,000 businesses, some of which were without power for more than three days.

Indicating how they could target AI infrastructure in the future, the group claimed responsibility for the Berlin attack in a letter called "Cutting off power to those in power," in which they said they carried out the attack to "cause significant damage to the gas industry and the greed for energy," as they believe that "in the greed for energy, the earth is being depleted, sucked dry, burned, ravaged, burned down, raped and destroyed."

Data Centers and Water Stress in the U.S.

Data centers are being built across the United States and globally, many in areas experiencing or projected to experience high water stress. The map below overlays major data center construction on top of water stress levels in the United States, helping to visualize areas which could face backlash from environmental activists.



Note: Future projected water stress under an SSP 3 RCP 7.0 pathway scenario in 2050
Source: World Resources Institute, S&P Global, Aqueduct 4.0, RANE Analysis

Labor Unions

Amid mounting fears about widespread job displacement and uncertainty about the future makeup of many industries, some labor organizations could launch anti-AI campaigns that push for improved working conditions and potentially involve strikes or other work stoppages. This could involve pre-existing labor groups and unions that tackle AI as a salient issue or it could spur the launch of entirely new labor-rights groups entirely focused on AI.

Labor activism traditionally relies on strikes, work stoppages, picketing and unionization drives, but increasingly includes whistleblowing, data leaks and online information campaigns exposing harmful technology deployments. AI has already played an early role in many unions' actions. Some have gone on strike while others have struck deals to avoid work disruptions.

For example, in January 2025, the International Longshoremen's Association avoided a major strike and reached a six-year contract agreement covering 45,000 workers at East and Gulf ports that includes a 62% wage increase over a six-year period and strict protections against fully automated port technology, serving as an early indicator for how the issue may be dealt with in some sectors.

Disgruntled Employees and Insider Threats

Galace also tells us that growing anti-AI sentiment among employees and "opposition to AI will also drive insider threats, including by those aggrieved with or fearful of being laid off and by those who disagree with their organization's adoption and/or use of AI tools." This is especially true as hackers are already exploiting growing AI

grievances among employees, as well as economic uncertainty, to recruit insiders for access to corporate networks or exfiltrate sensitive data on their behalf.

In addition to insider threats, employee activism can also cause reputational or operational challenges for organizations. For example, tech employees have already been central actors in AI debates, sometimes organizing petitions, walkouts and refusal-to-build campaigns targeting AI systems used for surveillance, warfare or mass automation.

Creatives

Creative communities have been among the most vocal critics of generative AI due to concerns about copyright infringement and the replacement of creative labor. Artists, writers, filmmakers and similar creatives have been among some of the first to mobilize against AI. For example, the Screen Actors Guild - American Federation of Television and Radio Artists initiated a historic strike from July to November 2023 over AI use in the industry and contract issues. Other forms of activism from these communities also include lawsuits over intellectual property as well as coordinated boycotts and public advocacy campaigns targeting AI companies.

Concern over AI stealing work from creatives has also previously spurred hacktivist activity. For example, in July 2024, hacktivist group NullBulge targeted the AI and gaming sectors, claiming to have leaked 1.1 terabytes of Disney internal data, including code, raw images and employee Slack communication in retaliation for Disney's approach to AI.

Activism from creatives and leaders in the entertainment industry can have far-reaching implications, given the platforms and influence that many of these high-profile individuals have. As such, creatives are highly effective at shaping public narratives through cultural influence, viral media and online organizing, making them important amplifiers of broader anti-AI sentiment.

Source: Reddit

Antitechnology Movements

Antitechnology movements are rooted in skepticism toward technological acceleration and the potential social and environmental harms of digital surveillance. This casts a wide net and includes concerns about surveillance and societal dependence on technology that erodes human self-sufficiency or human nature at large. Some factions draw ideological inspiration from neo-Luddite thought, arguing that certain technologies fundamentally undermine human autonomy and social stability.

This ideology has led to violent acts in the past, most notably by Ted Kaczynski, whose antitechnology and neo-Luddite views are often grouped under the broader category of environmental extremism, but in fact represent a distinct ideological movement that is becoming more salient in an increasingly digitized world.

As AI becomes more deeply embedded in society, a growing segment of the population becomes not only fatigued by low-quality AI-generated "slop" but also increasingly radicalized under uncertain economic conditions and labor prospects, evolving global norms and far-reaching cultural shifts, creating conditions that expands this movement's appeal and makes it more likely that it will draw new followers.

Kaczynski's manifesto, Industrial Society and Its Future, which argues that technology is a destructive force that regulates human behavior and restricts freedom and that violence is necessary to disrupt the technological system, may, in particular, be more likely to resonate in a period of rampant technological change. The ideology has been increasingly discussed online and several recent high-profile lone wolf attackers, including Luigi Mangione, the alleged killer of UnitedHealthcare CEO Brian Thompson, have drawn inspiration from Kaczynski.

Antiestablishment, Anticapitalist Groups

Anticapitalist and antiestablishment activists often frame AI as a tool that concentrates wealth and power among large technology corporations and governments. These groups frequently connect AI with mass surveillance and the concept of surveillance capitalism, worker exploitation and corporate monopolization of knowledge and labor. Growing wealth inequality and the view that large corporations and billionaires will be the primary beneficiaries of AI integration are helping fuel these groups' grievances, particularly as major AI firms are run by some of the world's wealthiest individuals.

Activism associated with these sentiments has historically included mass protests, property damage against corporate infrastructure, hacktivism and coordinated online campaigns, especially when technologies are viewed as reinforcing systemic inequality. Antiestablishment or anticapitalist hacktivists are among some of the most common (aside from those aligned with state interests, such as pro-Russian and pro-Iran hacktivists), with famous collectives like Anonymous largely aimed at challenging powerful institutions.

Human Rights Advocates

Human rights organizations have raised concerns about AI systems being used for mass surveillance, predictive policing, biometric identification and autonomous weapons systems. Advocacy in

this space typically focuses on policy reform, international regulation and public awareness campaigns, but can also involve strategic litigation, investigative reporting and digital transparency campaigns exposing abuses. In some contexts, activists may also coordinate global advocacy networks and information campaigns

Source: KQED

targeting companies that supply AI technologies to authoritarian governments.

Protest movements in this space also often target specific companies, at times involving employee backlash that can result in insider-threat activity or labor strikes and petitions. For example, in April 2024, Google workers staged sit-ins at Google offices in several locations under the banner "No Tech for Apartheid" to protest Google AI services being provided to the Israeli government and military, which resulted in the arrest of nine employees and the firing of over 50. More recently, in early 2026, over 1,500 Google employees signed a petition protesting expanded Google support for the U.S. Immigration and Customs Enforcement's (ICE) use of AI tools.

Digital Rights and Civil Liberties Advocates

Similar to antiestablishment and human rights advocates, digital rights organizations are more focused on privacy, surveillance, algorithmic transparency and data protection, arguing that AI can enable unprecedented monitoring and manipulation of populations. Such groups also express concern over AI's propensity to perpetuate biases and support other efforts to advocate for human autonomy.

These groups historically engage in policy advocacy, public-interest litigation, encryption advocacy and digital civil disobedience, including campaigns opposing biometric surveillance and automated decision systems. They also play a role in cyber activism through research disclosures, vulnerability reporting and public technical analysis of AI systems used by governments or corporations.

One notable example in this space is Austria-based data rights group NOYB, which has filed at least 22 legal complaints against AI companies for alleged violations of European data protection laws that it says infringed on individuals' fundamental rights.

Religious Groups

Some religious organizations raise ethical concerns about AI related to human dignity, moral agency and the perceived replacement of human creativity or decision-making. In certain traditions, AI is framed as raising questions about playing God and creating consciousness, spiritual authenticity or the dehumanization of society through automation, and in some cases, concerns about the heralding of end times.

Religious activism historically manifests through community organizing, moral advocacy campaigns and public demonstrations. Religious leaders often shape public opinion on emerging technologies through ethical guidance and institutional statements. While religious groups are less likely to sanction violent protest activities and instead will advocate for more peaceful measures to respond, such as boycott and divestment, religious sentiments on the topic could be more likely to radicalize lone-wolf actors to undertake action on their own, particularly if they believe AI is an existential threat to humanity or other extreme versions of AI risks.

Mental Health Advocates

How AI chatbots relate to mental health and the ability to influence the thoughts of vulnerable people is an increasingly salient topic. Mental health advocates highlight concerns about the sycophantic nature of some AI chatbots and their propensity to validate delusional beliefs or enable harmful behaviors, including those linked to self-harm and illicit substance use. Other concerns include AI-driven social media algorithms, deepfakes, digital addiction and the psychological effects of synthetic content environments.

Activism often focuses on youth safety, algorithmic transparency and regulatory oversight. These advocates typically engage through public awareness campaigns, research dissemination and policy advocacy, though their concerns can also catalyze broader public backlash against AI-driven digital ecosystems. Already, AI companies are facing several wrongful death lawsuits related to suicides, including multiple minors, and social media companies have gone on trial over the addictive nature of their platforms.

Source: Stopai

For example, in January, Stephani Gray, the mother of Austin Gordon, who committed suicide in November 2025, filed a lawsuit against OpenAI alleging that ChatGPT had been her son's "suicide coach." The number of ongoing mental health lawsuits against OpenAI is now at least 12.

Parents of affected children are likely to play a central role in advocacy efforts, which may be more likely to be effective in driving meaningful changes to how young people's use of AI is monitored. The historical precedent of Mothers Against Drunk Driving, instrumental in prompting federal action to raise the drinking age in the United States, supports this possibility.

What Are The Risks?

Protests and Physical Property Damage

Lichtenstein explains that anti-AI activism risks "could manifest in so many ways: physical violence, cyber disruptions, reputational fallout, financial costs, regulatory scrutiny, legal exposure, corporate competitiveness, employee satisfaction and effectiveness, financial valuations and otherwise." However, the most immediate risk posed by these social movements is the potential for physical protests, which may carry heightened risks of violence and property damage. This can take the form of not only protests outside of facilities, but also sabotage of corporate locations and efforts to disrupt AI-related supply chains.

According to Galace, "The likelihood of AI-related protests will only further grow as AI becomes more capable and accessible, facilitating its connection to a wider range of industries and issues, like environmentalism. This will not only fuel a rise in activism narrowly driven by opposition to AI, but will also heighten the likelihood and/or severity of activism opposed to the industries and issues increasingly connected to the technology."

Lichtenstein tells us that "Protests are more likely where AI intersects with different grievances: whether those be about job losses, environmental impacts, surveillance risks or otherwise." He adds that locations at particular risk include "areas with major concentrations of data centers, corporate offices of tech firms and those that have highly trumpeted the corporate rollout of AI tools and locations that are tech and/or activist hubs."

Moreover, this is a global risk, with Galace telling us that "physical demonstrations and hacktivism fueled by opposition to AI risk emerging in most countries, as employers and individuals worldwide increasingly adopt these tools." He elaborates to say, "this is even more so the case given media and industry reports suggest some companies are increasingly using AI to justify layoffs, regardless of whether or to what extent AI played a meaningful role in such decisions."

The likelihood of AI-related protests will only further grow as AI becomes more capable and accessible, facilitating its connection to a wider range of industries and issues

Insider and Cyber Threats

The primary cyber threats for organizations to consider are malicious insiders and hacktivism, as well as cybercriminals and nation-states seeking to exploit AI grievances. Insider threats can have both cyber and physical components. As Galace puts it, "These

insider threats risk manifesting in a wide range of ways, whether as disgruntled employees crippling digital infrastructure or leaking sensitive corporate communications and data, to employees pursuing physical violence against those they perceive responsible for the decisions with which they disagree."

Lichtenstein echoes this sentiment, saying, "Internally, there are a range of insider threats, ranging from employees aggrieved at corporate use of AI who may seek to physically or digitally sabotage systems, leak sensitive information to shine a negative light on the corporate use of AI or provide initial access for hacktivists, cybercriminals or nation-state hackers to conduct a wide range of threat activity."

Lichtenstein notes that cybercriminals may seek to exploit the corporate rollout of AI, such as through targeting disgruntled employees for access, while nation-states may also "seek to steal AI-related IP, discredit corporate AI systems, escalate to carry out disruptive cyberattacks against corporate networks or otherwise."

On the hacktivist front, groups are most likely to retaliate through website defacements and distributed-denial-of-service attacks, which can cause small-scale disruptions to services and result in reputational damage, as well as hack-and-leak or ransomware attacks from more sophisticated actors. Data leaks not only cause reputational damage and dips in stock prices for targeted organizations but also heighten compliance costs from mandated regulatory filings.

Groups such as environmental activists, antiestablishment collectives and human rights advocates may seek to use data-leak advocacy as a way to pressure corporations. Additionally, as some hacktivist groups increasingly adopt cybercriminal tools amid growing online commercial offerings, there is a growing risk that such groups will pursue ransomware attacks against organizations as a way of sending a political message about their use of AI and imposing more significant disruptions and financial costs.

Executive Doxxing, Intimidation and Threats of Violence

Anti-AI activism may also target specific individuals, including executives and other high-profile figures associated with AI deployment or development. This is particularly true of antiestablishment or anticapitalist movements seeking to hold specific individuals accountable. This can include a digital component that involves such groups publishing personal information about executives and calling upon followers of their movement to take action or otherwise intimidate targets, particularly as doxxing can take a significant psychological toll on victims.

Galace and Lichtenstein both note that there is a risk of violent attacks from insiders. Lichtenstein tells us, "Violent threats to senior executives would also be on the table – either in the form of workplace violence or from an insider providing an external threat actor with information about an executive's whereabouts, routine or other useful targeting data."

Information/Online Mobilization Campaigns

Anti-AI activism can also take place online via digital campaigns to tarnish organizations' reputations and mobilize public action. These can take the form of disinformation campaigns aiming to erode a

company's public image, negatively impact its stock price and sabotage impending business deals. Online petitions or protest organization can also take place on these channels.

Such campaigns may also call for boycott and divestment, such as the ongoing #QuitGPT movement, calling for boycotts of AI chatbots. Google employees' No Tech for Apartheid, also more broadly referred to as No Tech for Oppression, Apartheid or Genocide, also calls on individuals to boycott products that militaries use for surveillance or targeting.

Similarly, backlash against the use of Palantir systems for targeting systems in Gaza and for ICE facial recognition practices led Storebrand, Norway's largest asset manager, and several U.S. universities to divest from Palantir, citing risks of "complicity in war crimes."

What Should Companies Be Thinking About?

Lichtenstein tells us that first and foremost, organizations should always assume that there will be backlash. He says, "Companies are effectively caught between a rock and a hard place: they can't ignore the benefits of employing AI and giving their competitors potentially business-killing advantages, yet at the same time they can't escape the myriad types of backlash that are only going to deepen."

Because of this, organizations can develop risk mitigation strategies by first understanding the drivers of anti-AI activism. This can help them to identify which areas of activism they will be most vulnerable to, whether centering on corporate strategies to lay off employees in favor of AI investment or defense contracts that involve the use of AI military applications, particularly in controversial conflicts.

Organizations should always assume that there will be backlash.

As Lichtenstein puts it, "Understanding which risks you're trying to mitigate against can help organizations then focus on the most likely threat actors." First, he says, "It should be acknowledged that backlash will befall any organization in any way linked to an AI-related grievance. This means it's not just large, high-profile multinational firms, but it could simply be a small company that adopts some sort of AI tool that leads to job losses and triggers community pushback or even violence from a disgruntled employee."

However, some organizations are at higher risk than others. Understanding how vulnerable the organization will be is a crucial starting point. Lichtenstein says these include "any tech firms that work in any way on AI development, hardware or otherwise; organizations involved in AI infrastructure (like data centers); consumer-facing firms (everything from retailers to financial services to hospitality firms) that widely and loudly adopt AI tools; companies that provide AI services to government agencies; autonomous vehicle and other firms that use AI in more publicly observable ways; firms that are often characterized as controversial (healthcare insurers, oil and gas firms, defense contractors, etc.) and adopt AI; and firms whose executives, regardless of internal corporate use, loudly trumpet the benefits of AI."

Once organizations have identified their level of vulnerability, Lichtenstein suggests they identify their risk tolerance. "From there," he says, "organizations should think widely about the varying interests of their distinct stakeholders… Knowing where each set of stakeholders generally falls (knowing there will always be divergent opinions within different groups) will give organizations an advanced understanding of how their AI policy choices could rankle different groups."

Additionally, organizations should consider which types of backlash they are most likely to receive, whether against environmental or privacy practices or something else entirely, which will then help them understand the threats they are most likely to receive.

Once this step has been taken, Lichtenstein says that "Mitigating risks comes down to effective corporate security policies, ranging from risk mapping to understanding an organization's key assets and personnel that need to be prioritized for protection to developing effective digital monitoring capabilities to know if your organization's name has been circulating online in ways that could propel threat actors to take action – violent or otherwise."

There are also more broad actions that organizations should consider. For instance, Galace says that "Transparency and communication on major corporate decisions linked to AI will help limit risks of insider and even external threats, as doing so will help ensure relevant stakeholders remain aware of the organization's evolving stance on the technology and potentially offer these actors opportunities to provide feedback."

This can trickle down to clear AI ethics and guidelines for employees to follow, helping to mitigate potentially harmful practices most likely to result in backlash. From there, contract clauses and non-disclosure agreements can help mitigate reputational risks for departing employees who may share sensitive information in online mobilization campaigns.

General security practices, such as investing in data broker deletion services and monitoring employee activity for insider threats, can also help mitigate risks of executive targeting and data theft.