Beazley Logo

Article

The high stakes of high tech: An evolving anatomy of asset and executive risk

Chris Parker, Lucy Straker • May 27, 2026

Our Risk & Resilience report ‘Spotlight on Cyber Threats and Tech Advances 2026’ looks at the new cyber reality. Read on for Chris and Lucy’s insights on the physical risks that come with new media platforms and AI acceleration.

The timeline of public dissent has collapsed. AI-enabled “influence operations”[1] that weaponise deepfakes, synthetic media and coordinated misinformation have grown more sophisticated, accessible and realistic. Meanwhile, the immediacy and amplification across social media can mobilise crowds at speed. Collectively, this is accelerating the pace of online narratives tipping into offline action.

Concurrently, advancing technologies and booming data centre demands are fuelling public anxiety, and online hostility has fast transitioned into physical threats against tech infrastructure and executives.

This all adds up to a more volatile operating environment for businesses and industries, where digital drama culminates in costly impact on their people, properties and profits.

Offline risk at online speed

Across continents, Gen Z has weaponised the lower online barriers to collective action to propel political dissent and major systemic change, even collapsing governments in 2024/25 in Bangladesh, Nepal and Madagascar[2].

Meanwhile, incidents of mass anti-social disorder such as that in Clapham, London[3] were attributed to social media ‘link up’ trends driving loosely organised gatherings[4] that impaired local businesses.

This exposes a sharp pattern of online hype converting to boots on the ground with efficiency and speed, rendering companies blindsided and defenceless to sudden disruption, and assets, staff and operations left highly exposed.

Operational risk in a post-truth era

Social media can be an incubator for conspiracy theories and extremist debate. And with algorithms exacerbating false narratives, people react with physical urgency, many times before factual responses or containment measures can catch up.

In the UK, inaccurate claims regarding criminal incidents saw demonstrators targeting specific locations, such as hotels[5]. By the time official corrections were issued, the physical damage – vandalism and disorder – was already done.

And now, generative AI is making it much easier and more accessible to produce high-fidelity deepfakes, cloned audio and persuasive text at scale. Fallacious narratives spread fast and seem more credible, which can heighten tensions and public reach to escalate greater real-world incitement.

The violent turn of AI opposition

AI is both a tool for unrest and its target. Data centres, the physical backbone of AI and the digital age, are increasingly tied to environmental and economic strain. One fifth of the UK public believe AI concerns will provoke civil unrest[6], and already, cases of mounting political pressures[7] and direct protest are surfacing worldwide[8]. For data centres, physical incidents such as vandalism, arson attempts and nearby blockades can extend beyond physical damage and into material operational disruption.

This unrest has since turned personal and violent with reports of armed attacks on the homes of OpenAI CEO Sam Altman, and an Indianapolis councilman following a data centre approval in his district[9]. These signal a dangerous shift. Figures associated with technological infrastructure are now being targeted for the industries they represent, moving the threat from the boardroom to the front door.

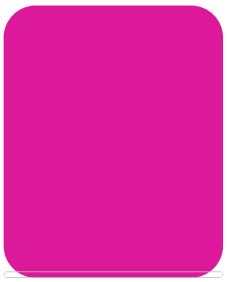
Securing physical resilience in a digital age

The intersection of rapid coordination and falsehoods, and AI and tech resentment are spurring more frequent, dangerous and costly civil unrest, fundamentally altering modern risk. Businesses should not wait to be caught in the crosshairs of chaos before assessing their exposure.

Existing insurance policies that cover property and liability may fall short. More specialist standalone policies such as Deadly Weapons Protection (DWP) and Strikes, Riots and Civil Commotion (SRCC) are designed to help firms stay on the front foot of such events.

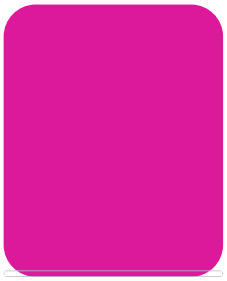
SRCC can protect businesses against losses and liabilities arising from physical property damage and business interruption. DWP addresses more weapon-specific risks through a combined framework of preventative services, crisis response support and insurance indemnification.

Amidst a rising tide of unrest, effective policies provide a more considered approach, helping organisations to not only recover financially, emotionally and reputationally after an incident, but also aid in strengthening their preparedness and operational resilience beforehand, and their response capabilities during and after.



Chris Parker

Head of Terrorism and Deadly Weapons Protection



Lucy Straker

Focus Group Leader - US Political Violence & Deadly Weapons Protection

1. https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-uk-general-election
2. https://www.theguardian.com/global-development/2025/dec/30/gen-z-protests-corruption-five-activists-nepal-madagascar-togo-kenya-morocco-protesters
3. https://www.independent.co.uk/news/uk/crime/met-police-crack-link-up-online-tiktok-trend-clapham-london-b2950408.html
4. https://www.standard.co.uk/news/crime/met-police-warning-arrests-youths-mayhem-clapham-high-street-london-b1277360.html
5. https://www.bbc.co.uk/news/articles/c9370jqxy18o
6. https://www.linkedin.com/posts/activity-7463176525388095488-CvhF/
7. https://www.news5cleveland.com/news/politics/ohio-politics/as-more-ohio-towns-ban-data-centers-lawmakers-move-to-study-impacts
8. https://www.theguardian.com/commentisfree/2026/apr/12/the-guardian-view-on-ai-politics-us-datacentre-protests-are-a-warning-to-big-tech
9. https://edition.cnn.com/2026/04/17/tech/anti-ai-attack-sam-altman

Home

©Beazley Group | LLOYD's Underwriters