

Year in Review: The Threat Trends of 2022 & Risks to Track in 2023

For businesses in all industries, 2023 means new ambitions, goals, and opportunities – though, with each opportunity, the New Year also brings new risks. To help Clients prepare for the unknown hazards of the year to come, Polaris has revisited the key stories and critical headlines of 2022, to identify and outline trending threats and emerging concerns.

Historic Protests Follow the Overturn of Roe v. Wade

- **2022 in Review: Protest Activity Consistent Since June 2022 Decision** – On June 24, 2022 – following months of speculation – the Supreme Court officially overturned Roe v. Wade, and, with it, Americans’ constitutional right to abortion. The decision triggered a wave of anti-abortion legislation in Republican-controlled states; as of reporting, abortions are largely banned in thirteen (13) states, including Texas and Louisiana. ([NPR](#); [New York Times](#).) The decision and subsequent restrictions prompted nationwide protests, including notable demonstrations outside the Supreme Court, and at the homes of supporting Justices. Unrest continued through the rest of the year, as pro-abortion protesters responded to developing state abortion restrictions, relevant litigation and legal challenges, and controversial individual cases. ([New York Times](#); [Al Jazeera](#); [Time](#); [CNN](#); [CNBC](#); [NPR](#).)
- **Looking Ahead: Further Protest & New Legal Challenges Likely** – Protests are already planned for the new year: anti-abortion group March for Life will emphasize “Next Steps” during its annual rally on January 20, 2023, which has historically seen counter-protest. Given the change in laws, this event may serve as a considerable tension point – especially as the pro-life event was attended by members of the alt-right group Patriot Front last year. ([March for Life](#); [American Catholic Tribune](#); [NBC News](#).) Beyond this protest, legal challenges to state abortion laws will continue; the Brennan Center reports that 34 lawsuits across 19 states remain pending as of December 19, 2022. As these cases are disposed, they may be met with additional protest. ([Brennan Center](#).)

Violent Backlash at LGBTQ+ Events

- **2022 in Review: LGBTQ+ Groups Face Violent Backlash, Protest** – Anti-LGBTQ+ violence is on the rise; a June 2022 report from the Department of Justice found that lesbian, gay, and bisexual individuals faced “significantly higher” rates of violent victimization than straight individuals. ([Department of Justice](#); [Human Rights Campaign](#); [NBC News](#).) This trend culminated in the tragic Club Q shooting, when a suspect killed five (5) during a November 2022 Colorado Springs drag show. Indeed, drag shows were a common target for far-right groups like the Proud Boys, White Lives Matter, and Patriot Front, who accused attendees of “grooming” children, and disrupted events in Ohio, Florida, New York, and elsewhere. ([Anti-Defamation League](#); [NBC News](#); [NBC NY](#); [PBS](#).)
- **Looking Ahead: Courts, State Lawmakers Likely to Continue to LGBTQ+ Challenges** – Legal challenges to gay, lesbian, and trans rights continue to generate tension and protest. On December 13, 2022, President Joe Biden signed the Respect for Marriage Act, which protects same-sex and interracial marriages at the federal level – though legal challenges to LGBTQ+ rights persist. Indeed, as soon as the Act itself was passed, Republican representatives sought to “defund” it, with critics claiming that the bill fails to “protect religious liberty.” Liberal critics, meanwhile, claimed that the law did not go far enough, as states may regain discretion over the legal status of gay marriage if the Supreme Court reverses its 2015 decision in Obergefell v. Hodges. To that end, lawmakers and influential jurists such as Supreme Court Justice Clarence Thomas have signaled interest in “reconsidering” the precedent, while as many as 325 anti-LGBTQ+ bills were proposed by Republican legislators in 2022 alone. These included Florida’s much discussed “Don’t Say Gay” bill, which led to considerable protest and criticism over the last year. As such, any new legislation affecting gay or trans rights will likely lead to further protest. ([NPR](#); [Fox News](#); [Politico](#); [Axios](#); [Washington Post](#); [ACLU](#); [CNN](#); [CNBC](#); [Bloomberg](#); [UN High Commissioner of Human Rights](#); [ABC](#); [PRISM Reports](#).)

This briefing was prepared for informational purposes only by Polaris Corporate Risk Management (“Polaris”). Please note that Intelligence Reports – though rooted in a historical review of past events and relevant current intelligence – are based partly on prediction; they are meant to anticipate potentially credible threats to a particular person, entity, or location at a particular point in time. As such, any reported threat vector or risk is inherently uncertain and speculative; any reported risks may not ultimately translate into tangible dangers, and other, unanticipated risks may still arise. Polaris deploys custom intelligence monitors, targeted geofences, and expert Boolean searches to screen for new and urgent content. Analysts take care to assess the objectivity or validity of each source – even as briefings may include partisan sources, given Polaris’ reliance on locally-sourced content. Polaris’ Analysts take care to mark any such content as it appears in the context of the report, so as to alert to potential biases. Polaris screens for relevant third-party commentary, including chatter by local social media users, reports from domestic news correspondents, and accounts from local assets on-the-ground, when appropriate. While Polaris Analysts will attempt to corroborate any reported chatter, these sources are inherently more speculative, and should be approached with a critical eye. Any unauthorized transmission, reproduction or communication regarding this report or its contents is strictly prohibited without the written consent of Polaris. Should this report or its contents be distributed to a third party, Polaris assumes no liability for any use, application or representation of the information herein. The reader understands that any statement by Polaris does not qualify as recommendation, endorsement, opinion or advice – even those statements relating to financial, regulatory or legal information – and that this document should not be relied upon as such under any circumstances or conditions.

Attacks on Critical Infrastructure

- **2022 in Review: Attacks on North Carolina, Oregon, & Washington Power Grids Cause Outages** – A January 2022 report from the Department of Homeland Security’s (“DHS”) Office of Intelligence & Analysis found that domestic extremists had “developed credible, specific plans to attack electricity infrastructure.” In the months that followed, the DHS’ warnings proved prescient: tens of thousands of North Carolina residents lost power following gunfire attacks on two (2) substations on the evening of December 3, 2022, while at least six (6) incidents have been reported at Washington and Oregon power stations since late November. Despite investigations from local authorities and the FBI, the perpetrators’ motives and intentions remain unclear – though the DHS previously warned that detailed, “low-tech” attack strategies were often traded among extremist groups in online forums. Despite a lack of clear motive, this string of deliberate attacks has only reinforced the DHS’ claims that online groups may be targeting electricity infrastructure. ([NPR](#); [Associated Press](#); [CNN](#); [The Guardian](#); [ABC](#); [Oregon Public Broadcasting](#); [Forbes](#); [KIRO7](#).)
- **Looking Ahead: Further Attacks Likely; Strategies for More Secure Infrastructure Needed** – Given the DHS’ warnings, and the increasing frequency of relevant incidents, attacks on critical infrastructure are likely to continue into the new year and beyond. Indeed, the DHS reiterated its January 2022 warning as recently as November 30, 2022, when it listed critical infrastructure as one (1) of many possible targets for future violent attacks in a National Terrorism Advisory System Bulletin. Given the costly, destabilizing nature of power grid attacks – with damages rising as high as seven (7) figures, and outages lasting for days or weeks – energy providers should consider proactive security methods. Measures might include a dedicated onsite security presence, a security assessment targeting potential structural improvements, or – given extremists’ use of online forums to disseminate attack strategies – detailed intelligence monitoring, to identify chatter targeting relevant sites. ([Associated Press](#); [DHS](#).)

International Conflicts Generate Domestic Protests, Disrupt Supply Chains

- **2022 in Review: Issues in Iran, China, & Ukraine Impact US Citizens, Supply Chain** – 2022 was marked by domestic gestures of international solidarity; Americans demonstrated in support of Chinese citizens as they protested their government’s strict “zero-COVID” policies, and Iranians, who rallied in large numbers following the death of a 22-year-old Kurdish woman at the hands of morality police. Most notably, however, were marches and fundraisers held in support of Ukraine following Russia’s invasion of the country in early 2022. ([ABC7](#); [CBS](#); [NBC News](#); [Wall Street Journal](#); [New York Times](#); [CNN](#).) While these demonstrations offered moral and financial support to those abroad, US citizens were themselves impacted by these conflicts in indirect ways: experts have noted that the Russia-Ukraine conflict, and global instability, generally, have worsened already-volatile supply routes, necessitating changes to the sourcing, transit, and delivery of key goods. ([MIT](#); [HIS Markit](#); [World Economic Forum](#).)
- **Looking Ahead: China’s Reopening, Continued Russia-Ukraine Conflict Prompt Supply Chain Fears** – After three (3) years of COVID-induced disruption, the US is well-poised to import goods – even as existing supply chains remain inconsistent, with foreign exporters facing new issues. While zero-COVID was unpopular among Chinese citizens, its absence meant a swift uptick in local cases. In the coming months, China – and, with it, the global supply chain – will likely face further COVID-related disruption. ([Fortune](#); [Barron’s](#); [Forbes](#).) Meanwhile trade routes and raw materials in Europe will remain unsettled as long as the Russia-Ukraine war continues – and given recent, deadly strikes in both countries, no immediate end is in sight. ([OECD](#); [CNBC](#).)

Rapidly Developing Cybersecurity Threats

- **2022 in Review: 2022 Continues Troubling Cyber Risk Trends** – The massive, high-profile cyberattacks of recent years – from 2021’s Colonial Pipeline and Log4J attacks, to breaches of Equifax, JPMorgan, and more – have made modern businesses all too aware of the disruptive potential of a breach. The pace of development is staggering: consider the Log4Shell bug, which, despite consistent patching and monitoring throughout 2022, may still pose a risk to systems running unpatched versions of Apache Tomcat server software – once representing 40% of downloads. Despite rapid, developing defenses against Log4Shell – or similar schemes – state and non-state actors were exploited throughout the year. ([Purplesec.us](#); [Wired](#); [InfoSecurity Magazine](#); [Politico](#).) The Biden Administration and expert partners/agencies have passed laws and published guidance to enhance attack preparedness and attack mitigation – though such measures require on enterprise attention and cooperation. ([CISA](#); [The White House](#).)
- **Looking Ahead: Tightening Regulations Demand Cyber Risks** – The increasing ubiquity of cyber breaches demands a regulatory response – and 2023 is poised to bring significant changes to federal or state compliance and cybersecurity standards. The SEC has already announced amendments to its governance, risk management, and incident disclosure requirements, while at least forty (40) state legislatures have considered new laws recommending or promoting robust cybersecurity programs within the last year. Regardless of whether these regulations impact your company however, all businesses face mounting consumer and partner pressures to protect their sensitive information, whether through employee trainings or rigorous risk monitoring programs. ([National Conference of State Legislatures](#); [Reuters](#).)