

Navigating Corporate Security Through Times of Chaos

Corporate security groups continue to be stretched thin, juggling multiple priorities within a constantly evolving environment. Risks have been non-stop since the 2020 election, compounded by protests related to the pandemic, social justice issues and economic unrest. As these priority issues become monitoring requirements, new threats have appeared to conflagrate matters further.

The ongoing effects of events like the overturning of Roe v. Wade, COVID-19, geopolitical conflicts and the many tragic mass shootings are now priority items alongside monitoring threats against executives, assets and business operations. With so much to consider, risk leaders must also consider the best way to protect their organization regarding reputational risk.

As we advance toward mid-term elections, the polarizing cultural landscape doesn't seem to allow more bipartisan discussion. So, what should security professionals consider when navigating the risks in the wake of extremism, unrest, and polarization?



Technology as an enabler to minimizing organizational risk

Regardless of what’s happening in the world, risk leaders are essential to supporting organizations in avoiding business disruption, ensuring operational effectiveness and maintaining regulatory compliance. Technology is critical to accomplish this and keep up with the rapid pace at which threats evolve.

However, you must ensure you have the right technology in place and that you’re not using a wide variety of solutions. Unifying your threat database, data sources, research tools and existing systems and workflows provides a holistic view of the end-to-end threat landscape, enabling teams to work efficiently to monitor and mitigate risks unique to your company.

Strategic adoption of technology that allows for shared research also will enable you to optimize your team’s research capabilities and efforts with **integrated search tools** in one place for a comprehensive view of threats, informed assessments and thorough investigations.



AGILITY

Act with speed and dexterity



CLARITY






Lead with crisp, informed decision-making



VISIBILITY

See with the broadest perspective

Here are some typical issues that security teams face and how a modern cloud-based platform, like Ontic, can assist in anticipating and reducing **corporate liability** during unprecedented times of chaos.

CURRENT STATE OF PROGRAM	CONSEQUENCES OF CURRENT STATE
Team members spend time between multiple, disconnected tools trying to connect data points	 Time is wasted jumping between tools attempting to piece together a holistic picture.
There’s a low level of confidence in the awareness of all potential threats.	 The threat landscape is growing and important signals are being missed.
Your data is stored in multiple places and there is limited visibility across the organization (HR, legal, cyber).	 It’s unclear what tasks have been completed and what to do next.
It’s impossible to monitor all the activity and identify the signals that need attention.	 There is no confidence in being prepared to act quickly to mitigate risk and avert incidents.
There are too many sources of potential threats to monitor and it’s hard to keep up.	 Missed threats due to lack of cohesive command, control, communications and intelligence (3CI).

While having the right technology in place is important, there are a few other tactics corporate protectors can put into practice when it comes to hot-button political issues and social unrest. On a practical level, here are a few suggestions to consider:

7 Practical Considerations for Security Teams

- 01 **Review protocols that are currently in place.** Now is the time to review emergency action plans, baseline threat assessments and communication protocols and keep the information flowing amongst teams.
- 02 **Identify key stakeholders.** Cultivate relationships with critical partners in your organization to stay in the loop about the organization's current public stances and any upcoming changes.
- 03 **Understand your baseline and monitor changes.** Be sure your strategic risk assessment has been updated recently to reflect any changes in your organizational structure and physical footprint. If you don't have one, now is the best time to create one.
- 04 **Take incremental action to protect personnel and assets.** As your baseline risk assessment changes, consider ways that you can ramp up your security posture in appropriate ways as the situation changes.
- 05 **Understand the proximity of threats to your physical footprint.** Consider the geographic regions that are most critical to your organizations and the tripwires that would be most likely to disrupt your operations in these areas.
- 06 **Consider second order impacts.** Ensure communications channels are open between security, legal and HR so all stakeholders can stay on the same page and respond quickly and appropriately to any emerging problems within the organization.
- 07 **Remain resilient, calm, and flexible.** Protecting executives and companies in this environment will take flexibility and adaptable processes.

FOR MORE INFORMATION PLEASE VISIT [ONTIC.CO](https://ontic.co)