White Paper: 2021 Civil Unrest Contingency Planning

January 12, 2021

Current Situation

- ***Alarming Violence at U.S. Capitol:*** The combined effects of a highly acerbic campaign tone, COVID-related election timing factors, and ongoing social unrest fueled by far-reaching disinformation culminated in the deadly January 6 attacks on the United States Capitol. New evidence suggests that the rioters' intentions may have been even more malevolent than initially understood—for example, online activity featured calls to kill Vice President Pence and Democratic House Speaker Nancy Pelosi.
- ***Further Violent Demonstrations Expected:*** Response to the uprising, most notably by social media companies that suspended President Trump and other right-wing accounts, is likely to invigorate an already-motivated extremist base even further.
- Not only are right-wing extremists threatening to return to Washington for a "Million Militia March" to disrupt Joe Biden's inauguration, but extremists may now be energized to incite violence closer to home.
    - The Boogaloo movement, a far-right and libertarian militia group, is advocating for gun rallies in all 50 states and D.C. to occur on January 17, promoting the event with a hashtag of the name of a rioter who was fatally shot at the Capitol.
    - The FBI reportedly first warned state and local law enforcement agencies of these January 17 plans in late December.
- ***Plan for Continued Unrest Beyond Inauguration Day.*** In October 2020, the U.S. Department of Homeland Security named Domestic Violent Extremists (DVE) as "the most persistent and lethal threat in the Homeland." Separately, December 2020 news reports indicated that the FBI had uncovered a DVE plot to attack the Southeastern power grid. We assess that the potential for civil unrest will apply well beyond Inauguration Day, as the country's highly polarized political climate endures.

The potential for violence in the coming weeks and months requires focused contingency planning by businesses across the country.

- Organizations must focus on ensuring that they have effective resources and process in place to **assess, mitigate,** and **monitor** risk from violent extremists. Addressing the risks present in this dynamic threat environment should be top of agenda for every executive with security and business continuity responsibilities in the country.

Assessing Risk: Understanding the Environment

Organizations should level-set on anticipating a volatile risk environment that can change rapidly based on:

- Evolving threat intentions;
- Vulnerabilities that come from either (a) physical adjacency to threat target, (b) supply chain dependencies, or (c) complexities from COVID-19 Work From Home (WFH) imperatives; and
- Downstream threat implications of business decisions (e.g., on political donations, account suspensions in the case of Internet and social media companies; policies on wearing masks).

Social media as a security enabler. While recent account suspensions by social media companies may change this, bad actors are indicating their intentions in the open with surprising frequency. This is evidenced by violent extremists' use of social media platforms to coordinate the January 6 Capitol building attack. Regardless, social media can also be an important early indicator of an escalating incident. But isolating credible threats from aspirational rhetoric can be a challenge for security professionals and businesses. Consider the following points:

- ***Data Gathering and Analysis.*** By using social media scrapers, key word algorithms and geofencing (to address both direct and adjacent threats), companies can establish filters and alerts to gather key threat intelligence for analysis. Intelligence feeds should gather information from a diversity of sources, as relevant accounts are active not only on traditional social media platforms, but also on targeted and unique social messaging platforms and the dark web.

- ***Insider Threat.*** Inappropriate social media activity can also be a concern when it comes to a company's own employees. This is not only critical for preventing workplace violence, corporate espionage, or other insider threats, but also to maintain awareness of incitement by employees online or their membership in violent extremist groups. While respecting privacy considerations, companies need a process for handling reports of employee social media posts of concern (e.g., the contain evidence of possible criminal activity).

Mitigating & Monitoring Risk: Maintaining an Effective Security Posture

Without effective preparation, well-resourced organizations can often find themselves ill-equipped to act when an event necessitates incident response activity. Key steps include:

Preparedness: Focus on categorizing high-value assets and applying graduated security measures based on risk. Key preparedness planning steps include:

- Plan for civil unrest contingencies, which could include: curfews; road closures; violent demonstrations and related attacks
- Ensure flexibility to enhance security measures based on threat information, with a particular focus on high-value assets
- For organizations or offices currently operating on site, review capabilities to secure site in event of violent demonstration (including tactical infrastructure, technology, and shelter-in-place and evacuation procedures)
- Ensure business continuity plans are updated and reflective of possible "loss of facility" events (can critical processes be transferred to another site? are failover plans and alternate worksite agreements in place?)
- Assume physical intrusions could also result in data breaches (e.g., via access to or theft of technology assets)

Situational Awareness, Incident Response and Crisis Management. Corporate entities should take measures to ensure that their security operations centers (SOCs) are poised to quickly classify and communicate relevant developments to security leadership. In turn, security leadership must be prepared

for immediate activation of incident response plans, as well as escalation to executive crisis management teams and law enforcement.

- Anticipate WFH risks for key executives and other employees (see below)
- Anticipate delayed law enforcement response due to competing priorities or resource constraints
- Address likelihood that insiders (an organization's employees and contractors) are a potential point of compromise

Law Enforcement Coordination. Establishing direct liaisons with local authorities in advance of a crisis or emergency is critical to meaningful information sharing and successful incident response—particularly because defending against a mob attack or large protest is beyond the capability of internal security forces.

- Corporate security programs should work closely with emergency responders and facilitate walkthroughs and trainings to enable swift response in the case of a crisis, such as an active shooter event or civil unrest activity.

Employee Training & Exercises. Companies should also consider how their own employees are trained to react in a crisis.

- If onsite, do they exit, or do they hunker down and, if so, where?
- Is Suspicious Activity Reporting training being actively provided?
- Of note: the C-Suite should be intimately familiar with their company's crisis response plans and should participate in executive-level physical security response exercises.

Physical Security Infrastructure. Ultimately, even with little to no intelligence or planning, a basic physical security infrastructure can prove decisive as a crisis unfolds – thwarting or even just slowing the progress of an attack.

- Protecting a company's assets can be a simple as prepositioning plywood boards to prevent damage to ground floor windows and doorways, or installing security bars at doorways to prevent breaches.
- Similarly, advanced access control devices such as vehicle barriers and bollards, security turnstiles, and elevator dispatch devices (to prevent unauthorized access to additional floors) can be instrumental in corralling attackers away from critical assets.

Testing and Audit. Organizations should test security systems (CCTV, access control, alarms, etc.) and inspect tactical infrastructure to ensure they are performing as intended.

Corporate Security Responsibilities in the Age of COVID

COVID-19 has shifted a large portion of the U.S. workforce, including business executives, from office to home. As businesses grapple with additional COVID-related security complexities, they should consider the following:

- ***Executive Protection.*** To be effective, executive protection programs depend on physical security plans that reflect the daily life of select public-facing executives, and these plans need to reflect that the "critical asset" has moved from the office to the home office.

- ***WFH Dispersed Operating Considerations.*** Just as executive protection shifted from the office to the home office, managers need to contemplate an expanded risk terrain for their employees. Organizations should consider providing the workforce with regular security updates and flagging local security situations to affected employees where feasible. People are a company's greatest asset, and plans and procedures should be in place to safeguard them from the increasingly dynamic threat landscape.

- ***Business Continuity & Resilience.*** Given the COVID-related dispersed work environment, and the elevated threat situation, leaders should ensure that critical personnel have designated secondary and tertiary decisionmakers to limit business impact. Key personnel should delineate the areas over which they have approval authority and business continuity managers should capture that content in plan documentation. Responders should also consider how response and investigations will be conducted in a manner that aligns, to the extent feasible, with mask and social distancing/WFH guidance.

Moving Forward

2020 witnessed civil unrest of greater frequency and magnitude, due in part to greater utilization of social media for mobilization and logistics planning. Prior to 2020, corporate security programs largely treated demonstrations as events requiring situational awareness and a light monitoring touch. However, we have observed how quickly events can devolve into violence and destruction, with businesses either targeted directly or sustaining damage due to their proximity to other targets. Businesses must recognize this increasingly kinetic security environment, consider impacts to employees, customers, and business partners, and prepare accordingly.