Resilience is a Competitive Necessity: Why the Security Landscape Has Changed Forever

Courtney Adante, PRESIDENT, SECURITY RISK ADVISORY, TENEO
Jonathan Wackrow, MANAGING DIRECTOR & TENEO GLOBAL HEAD OF SECURITY

When these two authors reflect on global events since our last chapter in Teneo Vision 2020, we did not anticipate that a global public health crisis would have dominated the agenda for corporate leaders and thrown economies around the world into tumult. While our observations on continued cyber threat, social unrest, violence, and natural disaster held true, pandemic and health security risk reared their head in a most unanticipated way, confirming once again to always expect the unexpected. As a matter of fact, that mantra should be the foundational approach of any executive with an eye toward risk management.

2020 has exemplified how one silent and invisible threat can re-write the social contract, business best practices, and political and economic priorities on a global scale. While pandemic risk previously seemed to be science fiction fodder, enterprises, governments, and citizens around the world found themselves simultaneously developing, implementing, and enforcing new health security habits and norms, which for some was completely unchartered territory. A new calculus for navigating the public health, operational, and reputational risks of a global pandemic also emerged. From the clinical and epidemiological terminology like "r-naught" values, "co-morbidity," and "moving average" that have entered our vernacular, to the mental gymnastics of deciding whether a subway trip, grocery store run, or a meet-up with family and friends merits the associated exposure risk, we have all become risk managers.

"2020 has exemplified how one silent and invisible threat can re-write the social contract, business best practices, and political and economic priorities on a global scale."

This newfound role for corporate leaders necessitates a new approach towards business continuity planning and resilience. Unlike in the past, when organizations typically based business continuity planning on responding to an assortment of external threats, the events of 2020 make it clear that today's approach must set forth a framework and governance structure that contextualizes an organization's risk exposure based on its specific operations, locations, vulnerabilities, and business objectives and thus its ability to handle an assortment of external threats, as opposed to managing a register of external potential trigger events.

The dynamic and all-encompassing nature of the COVID-19 pandemic revealed the need for a more proactive, systematic, scalable, and multi-disciplinary approach to business continuity planning. While many companies previously tended to develop incident response and business continuity plans specific to particular threats or types of threat, such as terrorism, natural disaster or cyber-attack, such a reactive and "outside looking in" approach left many leadership and operational teams scrambling to implement and scale the appropriate strategies and responses specific to their workforces, facilities, and operations.

This became especially true as the threat landscape expanded beyond public health to include crime and public safety, civic unrest, and reputational risk. Thus, instead of building business continuity plans around specific types of threats, leadership teams must instead adopt a more holistic paradigm, driven by the organization's specific vulnerabilities, rather than the universe of external threats—an inside-out, rather than outside-in approach.

By mapping out the vulnerabilities intrinsic to a company's operations, employee demographic (in the case of COVID-19, "essential vs non-essential") geographic footprint, supply chains and third parties, personnel and business model, leadership teams will gain a more comprehensive understanding of all the strategic considerations and associated communications and operational responses that any business continuity or incident response plan will need to address. With those in mind, they may develop a set of generalized thresholds or triggers for response and corresponding strategic, operational, and communications considerations or actions. While such a framework may require additional expansion to reflect the nuance of specific types of external threats or conditions unique to particular business lines and facilities, it

ensures that the enterprise has a baseline ability to respond and flex to address a modicum of threats, varying in impact and likelihood. It also forces the leadership team to identify key challenges and considerations specific to mission-critical operations.

An "Inside-out" Approach

In the sections that follow, we apply this "inside-out" approach to outlining the key tenets of business continuity planning, and then we go on to identify and define the key phases of business continuity and associated elements that business continuity planning and documentation should address. While we draw upon learnings from COVID-19, we've ultimately expanded those learnings to the broader context of natural, manmade, technological, or operational failures or threats within the corporate environment.

Teneo Risk's model conceptualizes resilience as an enterprise or system's ability to recover and rebound from both "acute shocks" and "chronic stresses." Acute shocks refer to the severe impacts on an enterprises' core facilities and infrastructure, personnel, or technology systems, while chronic stresses test the enterprise differently, building over time, often outside the organization's physical boundaries. These more prolonged strains ultimately create long-term challenges for the company's operations and organizational culture.

In today's world, substantial and traumatic events can take the form of anything from climate change-related issues or natural disaster in the form of wildfires, floods, earthquakes, volcanic eruptions, and hurricanes, to a major health pandemic, or terror or cyber-attack. Alternatively, chronic stresses, such as economic downturns, high unemployment rates, sustained high crime rates, or insufficient mobility and transportation systems, tax an enterprise and its workforce slowly, creating vulnerabilities, which, when exploited by acute shocks, can paralyze and ultimately inhibit the organization's ability to fully recover without significant investment of time, resources, and both financial and human capital. Acute shocks may also lead to chronic stresses; for instance, the acute shock of the COVID-19 pandemic has inflicted chronic stresses on to companies, political systems, and the global economy alike as lockdown restrictions persisted, and citizens faced growing uncertainty, fatigue, and personal financial struggles.

Thus, enterprises already facing acute shocks, in turn charged with deploying and managing new health security measures and compliance with a patchwork of public safety regulations, soon faced the compounding challenges of chronic stresses. They had to ensure the health and safety of employees and physical assets in areas with sustained protest activity, while also addressing employee, consumer, and public outcry for social change and greater accountability. These compounding and evolving acute shocks and chronic stresses highlight the need for a business continuity plan and posture that enables a business to manage through new, unforeseen, and increasingly complex and multidisciplinary shocks and stresses. This necessitates a more holistic view of risk, derived from a company's intrinsic attributes and resulting vulnerabilities, rather than focusing more heavily on external threats.

The Resiliency Test

Broadly, a given system's resiliency hinges upon its inhabitants' cohesion. For a company that depends upon its workforce and associated organizational culture, equally important – if not more important than rebuilding buildings, restoring utilities, and repairing infrastructure – is the resolve and willingness of an organization's people to weather both acute shocks and chronic stresses and come together and rebuild, despite an oftentimes painful recovery period. Therefore, the organizational culture and communications that unite a company are just as important as the processes and infrastructure. Therefore, today's truly resilient organizations possess a strong culture, mission, vision, and set of shared ideals that mobilize, engage, and unify a diverse workforce, its consumer base, as well as its other stakeholders.

"Equally important – if not more important than rebuilding buildings, restoring utilities, and repairing infrastructure – is the resolve and willingness of an organization's people to weather both acute shocks and chronic stresses and come together and rebuild, despite an oftentimes painful recovery period."

Answering the Challenge

Resiliency planning should take into account three main objectives:

1. risk assessment, proactive monitoring, and identification;
2. mitigation and agile response; and
3. forward-looking planning.

These three objectives ensure resilience is a continual process, in which anticipatory intelligence—in addition to considerations of an enterprise's unique, internal attributes—figures heavily into future planning. Developing an appropriate governance structure to set standards and provide relevant oversight for the resiliency planning process is key. In order to address the evolving scope of external threats and intrinsic vulnerabilities, the individuals who spearhead and oversee resiliency planning must represent each of a company's cross-functional teams and understand how to make planning and intelligence actionable. Because of the complexity and interconnectedness of various types of shocks and stressors, addressing risks to both traditional physical structures and the growing ubiquity of "connected devices" via the Internet of Things (IoT) — as well as identifying unique ways to leverage the current operating environment and resources available to maximize employee and external stakeholder engagement, innovation, and sustainability — requires perspectives and collaboration from across the organization.

Resiliency development should assess an enterprise's ability to engage frequently, accurately, and transparently with a broad range of stakeholders in order to create a sense of shared ownership in outcomes and decisions. It should also develop a broad understanding of potential sources of acute shocks and chronic stresses to an organization's people, processes, and technologies; identify associated infrastructure and actions for mitigation and recovery with limited support from external organizations or stakeholders; and develop the data sets and platforms for continuously monitoring threats and vulnerabilities within the organization and external ecosystem of consumers, governing bodies, and third parties. Mindful of the importance that a company's intrinsic vulnerabilities play in the "inside-out" approach to resiliency, we note below key areas of focus in the risk assessment process.

- **Geographic segmentation:** Various geographies and locations may be impacted differently or for varying durations and with differing degrees of public sector support or regulation. As a component of the risk assessment process, companies should map out daily operating activities, functions, and geographies — along with interdependencies among people, processes, technology, data, facilities, third parties, and locations, to understand the impacts of localized or global shocks and stressors, and to define the scope of subsequent monitoring and mitigation strategies.

- **Geographic distribution:** Identifying single points of failure, lack of diversification, and resulting risk exposures is key to ultimately filling those gaps. Areas of geographic concentration around operating activities and function, or over-reliance on particular third parties, may inform business continuity planning, calling for the need to segment critical functions or create alternate locations, sites, and staffing plans. Broadly, companies should look to diversify their supplier bases, customers, and third-party service providers across geographies.

- **Current geopolitical tensions or other existing chronic stressors:** Understanding local and global dynamics may prioritize monitoring efforts and location-specific resiliency planning based on locations or operations facing existing or escalating environmental, political, or humanitarian crises or tensions. Against the backdrop of geopolitical "chronic stressors," shocks may be particularly acute—exacerbating existing issues or causing shifts in the balance of power between governments and constituents that would disrupt company operations, supply chains, or consumer bases.

- **Current physical security and cybersecurity vulnerabilities:** Understanding an enterprise's physical and cyber security posture may reveal areas that bad actors may exploit in the event acute shocks or chronic stressors create or compound gaps or divert key resources and attention away from securing them.

- **Workforce attributes:** Specific characteristics or qualifications of an organization's employees may hamper its ability to staff for critical operations or recruit talent in the event of acute shock or chronic stress. Issues such as ability to

work-from-home, access to transportation and childcare — as well as employees' potential concerns around health, safety, or company leadership — may increase potential perceived or actual risk exposures for particular subsets of an organization's workforce and jeopardize their ability to perform critical functions.

- **Consumer attributes:** Acute shocks or chronic stresses may impact demand for an organization's goods or services, change the ways that they are distributed to market, as well as the ways consumers interact with the organization's brand. In addition, acute shocks or chronic stresses may change consumer or public sentiments, requiring organizations to revisit their mission, vision, values, and how those are communicated externally.

Mitigation and Agile Response

Upon understanding the full spectrum of an organization's intrinsic vulnerabilities, companies must develop mitigation and response strategies which balance the need for an overarching, fully-inclusive, and widely applicable framework with the location and incident-specific nuances. To achieve the right balance, business continuity planning exercises should start with scenario planning—outlining high-level operational definitions for escalating "tiers" or levels of incident or crisis and associated operational and communications responses, designed to address the vulnerabilities identified during the risk assessment phase. To balance generality and specificity, operational definitions for such tiers should focus on escalations in the degree of a given incident's impact to the organization's operations and reputation. They should also address the inflection points or triggers, either internal or external, that will force a company to react, either activating the business continuity plan; exercising heightened situational awareness or activating specific incident response plans without activating the business continuity plan; or de-activating the business continuity plan and returning to normal operations.

For each escalating threshold or tier, preliminary planning should address critical operational actions to maintain critical operations and communications. Operational actions might include building redundancies in supply chains,

designating both physical and digital back-up locations, establishing relationships with relevant public agencies, ensuring proper insurance coverage is in place, and equipping the company network and employees for remote-work, both from an information technology and cyber security standpoint.

When it comes to forming a basis for scenario planning, as well as informing the operational and communications responses to a range of triggering stressors or shocks, we have provided an illustrative list of focus areas that companies should consider. Again, in keeping with the paradigm that prioritizes a company's intrinsic attributes, operations, and workforce—rather than the universe of highly varied and constantly evolving extrinsic threats—we outline below illustrative areas that scenario planning and mitigation steps should address, as well as associated guiding principles for navigating the dynamic and increasingly complex situations that compounding acute shocks and chronic stresses may create.

- **Employee well-being and safety:** COVID-19 created greater operational and reputational pressure and accountability on employers to create more robust support systems for employees. In fact, an organization's productivity, culture, and identity lie within its people—making their safety, sense of well-being, and comfort the pillar of maintaining business operations. As employers moved to support employees in procuring childcare and offering extended work-from-home to address concerns about mass transit, childcare, and school re-openings, COVID-19 set a precedent for prioritizing employees' mental and physical well-being in all aspects of business continuity planning and return-to-operations. To understand employees' needs, sentiments, and concerns specific to different types of scenarios, companies should consider implementing pulse surveys or opening lines of communication by which employees may make inquiries or provide feedback. While COVID-19 has made particularly acute the importance of individual employees' circumstances outside the office environment, these considerations are critical to weathering any type of crisis. Additionally, ensuring that employees and management teams have two-way communications may enable leadership to gain early warning of potential emerging issues, while also fostering more collaboration and a sense of connection long after the crisis ends.

- **IT/cyber infrastructure and security:** The COVID-19 pandemic foregrounded the necessity of remote-work infrastructure, as well as bad actors' propensity to capitalize upon externalities for their own ends, with pandemic-related cyber scams costing more than 18,000 Americans a total of $13.4 million since the beginning of the year. In addition to investment in remote-work infrastructure and virtual collaboration capabilities, companies must implement network stress tests, install endpoint protection and spam filters, and conduct comprehensive and continued employee training on cyber hygiene to ensure continuity of operations. In any type of crisis, employees working remotely on unsecured networks, utilizing legacy or non-employer-issued hardware, or exercising lower levels of cyber hygiene and inhibition increases a company's susceptibility to debilitating attacks.

- **Supply chain and global trade:** Developing an understanding of critical third parties—as well as fourth and fifth—and their vulnerability to acute shocks and chronic stresses and respective resilience programs will avoid back-up in operations and single points of failure. Mitigation plans should include strategies for in-house substitutions or contractual clauses in third-party agreements, prioritizing delivery of products and services to the organization over other clients or competitors. Enterprises should also work with counsel to review contracts for potential uncertainty in rates, payments, regulatory, or data-sharing requirements in the event additional work or servicing is necessary for continuity of operations. Additionally, understanding customers' access to services, delivery channels, and demands for products will inform strategic and operational priorities.

Pandemic-related cyber scams affected over 18,000 Americans and cost a total of

$13.4 million

In addition to prioritizing employees' physical health and safety, employers must also consider their mental health and wellness, workforce productivity, and issues unique to the C-Suite, as they lead the organization through crises. This pandemic crisis tested the resolve and leadership skills of the best executives. The leaders that resonated most

with employees, investors, and the media were those executives who demonstrated authenticity, provided transparency, and acknowledged the uncertainty of the situation while making hard choices about staff and operations. Those organizations that embraced the crisis as an opportunity found new ways to communicate and innovate in the face of adversity and identified improved ways of engaging talent and managing workforces through technology, new policies and procedures, and simple, open dialogue about the future of their businesses.

The patchwork landscape of state and local public health regulations against a backdrop of public health and federal guidelines during COVID-19 heightened the onus on the private sector to reconcile government guidance and enterprise decision-making. On a global scale, travel restrictions, as well as varying paces of re-opening recovery around the world, also forced enterprises to account for split workforces, subsets of which were working remotely, while others returned to or continued to work from offices. Executive leadership teams should understand broadly which sets of guidance take legal precedence, as well as the political dynamics underpinning relevant legislation or guidance. In turn, that guidance and legislation should serve as an input or factor in developing company-specific thresholds or triggers for company responses—such as restrictions on employee travel, in-office work, and other course-of-business activity—based on strategic priorities, geographic footprint, and employee needs and sentiments. Enterprises also need to understand how local or national level policies impact consumers and their access to or demand for goods and services. And finally, business continuity planning may also merit companies establishing liaison and communication with relevant local law enforcement, public health, or other government agencies. Such relationships may be critical for getting the latest information, resources, and advisory in the face of a crisis, as well as ensuring regulatory compliance or adherence to best practices.

The economic and operational challenges that COVID-19 has catalysed highlights the importance of understanding insurance coverage, as well as the entirety of a company's contractual relationships—particularly force majeure, termination, and non-performance clauses. Depending on the magnitude of the crisis and the degree of oversight, governments or regulators may also increase scrutiny, and employees may also demand greater transparency around the legal or privacy implications of company mitigation measures.

Forward-Looking Planning

Setting forth a governance structure and accountable parties for strategic decision-making, operational execution, and intelligence is critical to ensuring an enterprise's business continuity. An organization should designate an executive team, comprised of the CEO, CFO, and other C-Suite representatives from Security, Operations, Communications, Legal, Human Resources, Marketing/Public Relations, and Investor Relations groups—as well as back-ups for each of the primary representatives. To account for incidents requiring an operational response, a separate incident response team, often comprised of the deputies or operational staff of the executive team members, should be charged with carrying out the tactical or operational responses based on the executive team's decisions. Lastly, the company should consider designating a team dedicated to the communications response, to include representation from internal and external communications, public / media relations, investor relations, and digital / social media. Depending on the triggering incident and company operations, critical third parties, such as public relations agencies, external counsel, or other consultants performing mission-critical functions, should also be included on the response or communications teams.

Each of these teams or task forces—as well as their members' designated alternates—should be trained on their respective roles, with the executive team members prepared to execute timely decisions, determine whether or not to activate the response and / or communications teams, and convey those decisions to the right team for execution. Similarly, each member of the communications and response team should be designated a set scope of responsibilities related to carrying out those decisions. They should also be equipped to develop guidelines of policy expectations, frameworks for responding to, and escalating new information in ways that will meet the needs of the executive team and updating and maintaining the business continuity plan. Table-top exercises or simulations are one means of providing individuals training and also understanding points of coordination and interdependency between teams or functional groups and to assess the effectiveness of resilience and business continuity planning.

The Planning Necessity

Although we are unlikely to realize the full breadth and significance of the COVID-19 pandemic and its aftermath for years to come, it has already heightened the accountability placed on enterprises to place resiliency and business continuity as cornerstones of corporate policy, operations, and culture. It has also underscored the inescapable truth of life in the increasingly interconnected, fast-paced world: we will always be living with risk—and that risk can grow exponentially in complexity and impact—meaning that risk management and resiliency will become more focused upon mitigation than prevention. How quickly and effectively the leadership team responds to acute shocks, chronic stresses, or the combination of triggers that today's risk landscape presents will define an organization's success or failure. Thus, the table stakes of business continuity planning have been elevated to those of the largest and most high-profile transactions. Employee lives, in addition to the company's viability, depend on it.

As the public health crisis and its prolonged economic and political fallout illustrated, these times demand a new, more proactive, and cross-functional approach towards business continuity planning and resilience, which moves away from an "outside-in" model, in which leadership teams react to a laundry list of potential external threats, and towards mitigating risk from the inside out.

Drawing upon the illustrative areas of focus set forth here, companies must continue to look inwards—understanding how acute shocks and chronic stresses might exploit or test their specific operations, locations, consumer and/or investor base, workforce, and supply chains. Those dynamics, in conjunction with the strategic, operational, and communications responses and the governance and infrastructure that support and facilitate those responses, will form the backbone of a holistic resiliency model, which can flex and grow to meet the magnitude, complexity, and velocity of any number of threats. And in an operating environment where those threats are here to stay, systematic business continuity planning, vigilance, and preparedness are not only competitive advantages, but necessities.

"In an operating environment where those threats are here to stay, systematic business continuity planning, vigilance, and preparedness are not only competitive advantages, but necessities."