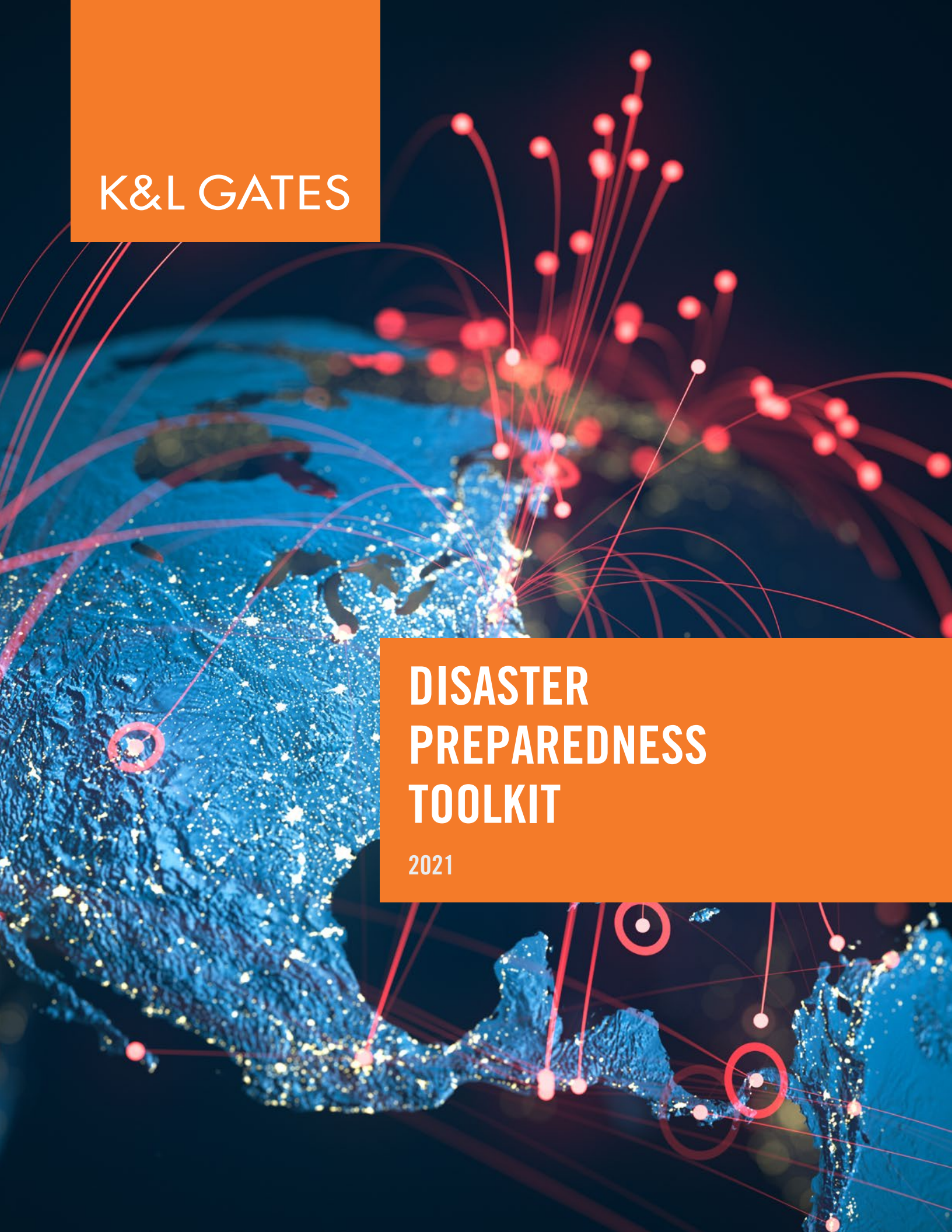
K&L GATES



DISASTER PREPAREDNESS TOOLKIT

2021

CONTENTS

YOUR TOOLKIT FOR DISASTERS OLD AND NEW

The Disaster Preparedness Toolkit is designed to help businesses assess important issues in planning for widespread emergency events. As we experienced throughout 2020 and through present day, natural disasters are among only some of the events that can lead to business disruption. Some disruptions may be short and their impacts quickly remedied—while others may permanently change the way business is conducted, such as what we witnessed as a result of the COVID-19 pandemic. In 2021, businesses must now be even more vigilant in guarding against and responding to ransomware cyberattacks, which carry to the potential to cripple entire industries.

Proactively preparing for various disasters, including mitigation efforts and emergency response procedures, is imperative to the successful navigation of a crisis. This updated toolkit is a resource to guide your business in planning for business interruptions and implementing continuity strategies.

COMMERCIAL CONTRACTS

The common law doctrines of impossibility of performance, impracticability, and frustration of purpose may be available to set aside contracts when an unforeseen event renders contractual obligations impossible to perform. Relying on common law doctrines, however, leaves contracting parties at the mercy of a court's interpretation and application of the doctrines to any given event. This creates uncertainty and may not properly allocate the risk arising from a natural disaster or other widespread emergency events such as wildfires or a pandemic.

One method to allocate and mitigate such risk is the use of a "force majeure" clause. "Force majeure" is a French term that is defined as a supervening force. The term is often used interchangeably with an "Act of God" despite the fact that a force majeure may be defined to cover more events, such as man-made events, and is a broader concept. Force majeure events are events that cannot be anticipated or controlled. A party relying on a force majeure clause must show that the event was unforeseeable, outside the party's control, occurred without its fault or negligence, and was the cause of the nonperformance.

Force majeure clauses are activated by the triggering event's impact on contract performance, not the event's impact on the parties themselves. Therefore, these clauses can be effective tools for businesses around the world. For example, if a party was contractually obligated to manufacture and deliver goods to a buyer and a natural disaster or war prevented the party from acquiring necessary parts for the goods, it could be prevented from performing through no fault of its own. A force majeure clause may mitigate such risk and, even when a party is all the way around the world, the clause may provide an opportunity to escape an otherwise economically disastrous event.

Drafting an Effective Force Majeure Clause

A well-drafted force majeure clause will excuse obligations under a contract where circumstances beyond a party's control create a delay in performance or a partial or complete inability for a party to perform. Force majeure clauses are interpreted under standard rules of contract interpretation. Parties may, and often do, have differing opinions as to what types of events should

excuse performance. As a result, overly general force majeure clauses run the risk of creating ambiguity, which may lead to litigation regarding whether an event falls within the scope of the clause. Therefore, parties should clearly define the term "force majeure" in their contract. This is typically accomplished by setting out an exhaustive list of specific events deemed to trigger a force majeure. A force majeure clause may, but is not require to, also include a catch-all phrase that provides clarity as to what other, if any, types of events will also be considered a force majeure under the contract (e.g., any events beyond a party's control, or only events similar to those specifically identified). Interpretation of catchall phrases varies from jurisdiction to jurisdiction, but they are generally interpreted narrowly, so parties should enumerate all specific events as to which they would like protection.

A well-drafted force majeure clause will further identify the effects of the various triggering events on each party's obligation to perform. For instance, parties should consider under what circumstances an obligation to perform under a contract is temporarily suspended and what force majeure events would cause contract termination. When parties specifically include language in their contract defining the effect, scope, and application of the force majeure event, that contractual language will control rather than common law.

Finally, a force majeure clause should include a notice provision whereby the party seeking relief under the clause must notify the other party. Force majeure clauses serve to properly allocate risk, but they should also serve to properly notify parties that performance will not occur as planned so that damages can be mitigated.

Application of a Force Majeure Clause

When a force majeure event occurs and prevents performance, the clause may be invoked to excuse the now impossible performance. This may be a complete excuse of performance, a delay in performance, or an allowance for partial performance depending on the individual circumstances. The party seeking relief from the performance obligation has the burden to prove that the force majeure clause should be invoked. Further, the inability to perform is determined based on an objective standard; it must be clear that no one could perform the party's obligations under the contract due to the event that has occurred. If the force majeure event does not affect the party's ability to fulfill any of their obligations and the contract can be performed normally, the force majeure clause will not be applicable. For instance, if a contract contains a force majeure clause that contemplates a hurricane preventing performance and a hurricane occurs but does not prevent performance, then the force majeure clause cannot be relied upon to excuse nonperformance. Similarly, the fact that a force majeure event makes performance more expensive is generally insufficient; the standard in most jurisdictions is physical impossibility of performance.

As mentioned above, in the days after a force majeure event, parties must also be prepared to provide notice in compliance with the contractual provisions. While the force majeure event may be well known, such as with hurricanes or a pandemic, formal notice will likely still be required to trigger a force majeure clause. Parties to commercial contracts should be aware of their contractual notice requirements. Notice deadlines can often be quite short and the failure to provide timely notice could result in the waiver of a party's contractual right to invoke their force majeure clause and the protections it provides.

Natural disasters and other widespread emergency events can disrupt virtually any business. COVID-19, civil unrest, hurricanes, and wildfires serve as reminders that these risks are unpredictable and potentially devastating. A well-drafted force majeure clause is a tool for parties to attempt to mitigate and allocate risks associated with such events.

COMMERCIAL REAL ESTATE

Commercial real estate ownership, occupancy, leasing, financing, and management comes with its recognized risks, largely economic and demographic in nature. Sometimes the risks are reflective of a long-term historical context of natural disasters occurring with some degree of frequency. An asset's perceived vulnerability or resiliency to a potential natural disaster has a significant impact on its use and value. Until recently, experience has been a good guide in risk assessment and planning for future natural disasters.

The current period of civil disturbances and a worldwide pandemic emergency have taken on a new urgency, however, forcing commercial real estate interests to conceive the inconceivable. We are now experiencing a disruption of the understood patterns and risks of real estate ownership and use on a scale not seen for generations. This paradigm shift serves as a warning to rethink how the commercial real estate industry anticipates and reacts both to human events and to natural disasters, and perhaps more importantly to reconsider whether to remain invested in an immovable asset that cannot adequately be protected from natural or human events by any measure of contractual protection.

Consider Risk Allocation Provisions

Sometimes terms in real estate agreements are carefully negotiated so that the contracting parties enter their commercial relationship with a full understanding of their respective rights and obligations as well as those of the insurance companies that stand behind each of them. Even so, competent and experienced decision-makers have been known to brush over risk-allocation provisions as being "remote" or "unlikely" to ever come into play. But the business risk that one party may decide to take may not be consistent with the level of risk tolerance of other parties.

For parties with widespread operations, an isolated casualty event that affects a single project may not present a difficult challenge. Even if the contract terms are not ideal for a party, it should be capable of bearing a loss from one affected real estate asset. If a regional or national disaster strikes, however, for the party with hundreds of locations under its ownership, care, or responsibility, the impact of haphazard contract negotiation or lack of attention to disaster preparedness could present major problems. On the Gulf Coast and Eastern Seaboard of the United States, hurricanes and major windstorm events have created this mass casualty effect. Other parts of the United States are not immune. The West Coast must consider the widespread impact that a major earthquake, volcano, or wildfire could create. The Mississippi River Basin must consider flooding. Blizzard events could affect any part of the United States that experiences cold winters. Defying true characterization, massive civil unrest, attacks on key infrastructure, or external military action could be added to the list.

Prudent business decision-makers at every level of the commercial real estate relationship must have a complete and realistic understanding of the risk-allocation terms of its contracts and leases as well as a general understanding of the rights and obligations of other parties that may not necessarily be in contractual privity but whose failure could have a material impact on the other parties. With credit to the adage that people learn best by doing, it is not only important for every party to have previously considered the theoretical "what to do" if the inconceivable occurs, but to practice it through drills. This involves learning by action—a tabletop drill that presents a pre-planned disaster scenario and a package of relevant existing contracts and

agreements to key personnel of the owner, manager, landlord, lender, or tenant (including the lawyers to help interpret the documents). The drill should allow the business to consider every conceivable resulting impact on itself and the other parties, and how to deal with it.

Asses Risk Tolerance With a Disaster Preparedness Drill

Imagine the possibility of contemporaneous natural events and how these events might affect critical elements of real estate ownership or occupancy—for example, a major coastal disaster evacuation effort coupled with violent civil unrest or infrastructure failures. Even if such a drill yields no feasible answer to preparedness, it may help to demonstrate the stark alternatives of "fight or flight" under potentially insurmountable circumstances while giving cause to reconsider risk tolerance and asset valuation and to exit a particular location or market.

When preparing the disaster narrative, try to imagine the worst-case scenario. When evaluating the disaster narrative, review the contracts to identify the terms and obligations that suddenly became relevant with the casualty event. These can include: (a) the notice requirements, (b) duties to mitigate damages (minimize losses and prevent further damage), (c) insurance coverage obligations, (d) the structural and operational issues that may render performance of the contractual obligation impossible and whether performance is excused by a force majeure clause, (e) what the default provision says about payment and performance obligations, and (f) contractual obligations when performance is impossible but not excused.

Try to drill down in applying the contractual terms to identify the weak points and issues. Even if you can perform, can the other parties? Is there a weak link or a concern that another party would not be able to meet its obligations, and what would that failure mean to each party on both an immediate and long-term basis? What should the company do, how should it react to the other players, and, more importantly, how should it respond to the immediate need for self-preservation? The contracts may not even address the issues.

The list below presents some matters that might be given consideration in preparing for and undertaking the desktop disaster preparedness drill:

- Is the party properly insured for mass casualty? What about deductibles or self-insurance, and coverage limits and exceptions to coverage? Is the insurer solvent and able to bear the collective claims arising from a widespread casualty?
- Is the party's financial condition solid? What about the other important actors involved in the chain of performance? Is there an identifiable "weak link?" Can that weak link be replaced easily if it fails to perform?
- Who bears the risk of loss in a casualty situation? Who is responsible for restoration? It may depend on whether it is a partial loss, a total loss, or how it was caused. How is that determination of causation of partial or total loss made, and what if there is a disagreement?
- Who gets control of insurance proceeds in a casualty situation?
- What if the insurance company is slow to pay casualty proceeds or refuses to pay proceeds based on "small print" in the insurance policy?
- Can a lender elect to apply proceeds to pay off the loan instead of applying to the cost of restoration or replacement?
- Can a lender elect to hold insurance proceeds for payment to owner, manager, landlord, or tenant only after full restoration was paid out of pocket?
- Can a party elect to terminate its contract if the casualty is bad enough?
- Is any party excused from performance following a disaster event? What does the force majeure clause include and, more importantly, what does it exclude?

- Who bears the risk of damages that may result from excused or unexcused failure to perform due to a disaster event?
- Does an operating agreement or management agreement address what happens if there is nothing left to manage?
- What happens if operational restoration of the property requires extraordinary measures that are outside of any contractual obligations to restore or replace?
- Are there backup plans for continuing business notwithstanding the loss of such things as logistics, delivery, and showroom, store space? What about generators, cash reserves, and sufficient staffing for emergency or "skeleton" operations? Will there be sufficient staffing for minimal security?
- What happens if a disaster affects an area but the property is spared, or a disaster occurs elsewhere but has a spill-over effect on other properties? Do contracts address indirect impacts or must the casualty have a direct impact on the operations?
- In addition to the obvious and direct impacts of physical casualty to the real estate facility, consider the potential indirect problems resulting from scarcity or loss of power or fuel; the inability to acquire inventory or supplies; or the inability of employees, vendors, or customers to get to or from the property. The loss of power or utilities—the breakdown of electronic equipment, internet, or cloud-based communications—can result in the inability to access critical data, to make payments to vendors or creditors (payment of rent, taxes, loan payments, or other obligations), or to process credit/debit card transactions. Other indirect impacts might include supply-chain disruption, looting, theft, and extreme price changes resulting from gouging or lack of supply in relation to demand. Not all of these may be covered by the standard force majeure clause or insurance.

Some of these considerations tilt toward that "worse-case" scenario, but even the worst conceivable casualty event might be eclipsed by the inconceivable. Thus, the list is not exhaustive and should be adapted to the needs of the organization and to the interests of each party. The answers for one party may be different from the others. When negotiating and drafting new contracts, the business decision-makers and legal professionals should try to cover as much as possible within reason, but be prepared to explain or to address problems that later occur outside of reason. When a contract or agreement fails to address certain issues, there should be some thought given to amending, replacing, or supplying inadequate or missing terms critical to disaster preparedness and response. The timing may not feel right to raise disaster preparedness issues anew with real estate partners, but it may be too late after a disaster strikes.

Limitations of Contractual Provisions

Current events have brought force majeure clauses and risk allocation provisions of many real estate contracts and leases to the forefront, often being tested and applied to circumstances beyond their intended limits. The practical limitations of even the best-prepared contractual provisions are being exposed and examined. Parties that believed, with good reason, that they had iron-clad contractual protection now are finding that such protection was illusory and impractical or impossible to enforce. In addition to giving careful consideration to the critical elements of contractual protection and logistical planning against a future natural or man-made disaster, recognition also should be afforded to the potential that no measure of protection may be adequate under the worst-case scenario and to assess that risk accordingly.

CONSTRUCTION

Construction projects suffer from significant but often underappreciated risks such as natural disasters, wild fires, and pandemics.

Those consequences may include: increased supply and labor expenses, costs associated with mitigation activities to protect the workplace, lost business income, environmental impacts, differing site conditions, and increased interest on loans. Parties to construction contracts should look toward customized contractual force majeure clauses and broadened builder's risk policies to allocate these costs.

Customize Your Force Majeure Clause—It Can Address More Than the Time to Perform

From a project's outset, the parties often agree to a contractual force majeure clause addressing only extensions of time for performance in the event of a force majeure event or the right to terminate for a party's failure to perform. In the wake of COVID-19, parties have begun to revisit force majeure clauses to address the financial consequences of a widespread emergency event.

For example, a natural disaster can increase the cost of materials for a project. In a fixed-price contract, the risk of increased material costs often rests with contractors, who might not be in the best position to absorb them. Contractors are increasingly seeking to have force majeure modified to address and allocate the consequences associated with these risks. These modifications can include a cost-escalation provision that allows the recovery of increased expenses pursuant to an independent cost index or another contractual formula. It can also allocate mitigation responsibilities to the party that will be in the better position to organize and decide appropriate mitigation actions to preserve the project, equipment, and materials. While it may be appropriate for the general contractor to manage the implementation of crisis management activities, the contract can provide specific procedures for allocating liability for the associated costs.

Add Endorsements to Builder's Risk Insurance Policies to Cover the Financial Impact of Natural Disasters

Builder's risk insurance covers a construction project during the course of construction and can function as a risk transfer mechanism. A policy can cover all parties with an insurable interest in the project, including subcontractors who will have an insurance interest in the work and materials they have invested in the project. While professionals in the construction industry may be familiar with builder's risk insurance in the context of losses to the actual project itself, a policy may be secured to provide broader coverage. Parties should consider adding endorsements or supplemental coverages to the builder's risk insurance policy to insure against the financial consequences of other emergency events.

The Insurance Services Office has created standard builder's risk forms, but most insurance companies do not use the standard forms—they use their own. As a result, the coverage varies from insurer to insurer. Well-drafted construction contracts will include a section addressing minimum requirements for insurance on the project. With respect to builder's risk insurance, at a minimum, this section should identify which party is responsible for securing the builder's risk policy; the scope of the builder's risk coverage, including endorsements or supplemental coverages for the financial consequences of emergency events; aggregate policy limits; maximum

sub-limits; maximum self-insured retentions or deductibles; and the policy period.

Consider solutions to mitigate the impacts of potential widespread emergency events at the inception of a project. Negotiating force majeure and builders risk insurance provisions can yield significant financial advantages in the event a widespread emergency event occurs during construction.

DATA PRIVACY, TECHNOLOGY, AND DIGITAL CRISIS PLANNING & RESPONSE

There is no denying that we live in a digital world. Businesses must think beyond the tangible ramifications and physical losses that may result from a crisis—whether it be a natural disaster, a data breach, or a pandemic. Instead, they must carefully construct and implement not only detailed policies and procedures, but also communications and emergency preparedness plans designed to avoid and manage the digital fallout from any crisis. Strong cybersecurity, information management, and communications policies and protocols can help a company not only survive a crisis but also emerge successful and stronger than ever.

The COVID-19 pandemic has accelerated digital transformation and fundamentally changed how we live and how we do business. The quick pivot to "work from home" revealed many weaknesses in businesses' critical infrastructures. Cybercriminals have had a field day working to exploit those weaknesses—we've seen a surge in digital attacks, especially ransomware attacks, which can and do have catastrophic affects on businesses in all industries and across geographical boundaries.

Some industries have regulations in place to ensure business continuity in the face of a disaster, such as the Health Insurance Portability and Accountability Act of 1996 for the health care industry, and the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act) for the banking and finance industry. Some states such as Massachusetts, have, for some time, had regulatory guidance in place that offers businesses with best practices for information management. See 201 CMF 17.00 (2009). California has been the leader, passing the first state-specific data privacy law in 2018.

The California Consumer Privacy Act (CCPA) has only been in effect since July 2020, but has inspired other states to follow suit. The California legislature has also inspired itself. Drawing inspiration from the General Data Protection Regulation, the California Privacy Rights Act (CPRA) was passed by California voters in November of 2020 and will go into full effect on 1 January 2023. The CPRA updates, expands, and strengthens the CCPA and has drastically increased the potential penalties companies and other organizations face for violations. While the CCPA provided a 30-day cure period, the CPRA does not permit entities to remediate issues during that period without facing lawsuits.

Other states have followed suit. For example, in February of 2021, Florida's governor put his support behind House Bill 969, a draft consumer privacy law that follows the lead of California's CCPA. If passed, the Florida Consumer Data Privacy Law would go into effect on 1 July 2022.

Florida is not alone—the Minnesota Consumer Data Privacy Act was introduced to the state legislature in February of 2021; the Oklahoma Computer Data Privacy Act was passed in the state House of Representatives in March of 2021; Virginia's Consumer Data Privacy Act passed in February of 2021; and New York introduced over **50 privacy bills** for consideration during the 2021-22 session, including two comprehensive privacy bills—Senate Bill **S567/A3709**, which includes rights similar to those established by the CCPA, and **A680**, which require companies to disclose their methods of de-identifying personal information, places special safeguards around data sharing and to allow consumers access to names of all entities with whom their information is shared, and creates a special

account to fund a new office of privacy and data protection, among other things.

In many cases, and where the bulk of states have not yet enacted consumer data privacy legislation, businesses are left to their own devices to establish and follow best practices to ensure they weather any storm.

Natural disasters and other crises do not discriminate. The failure to plan ahead can be catastrophic for any business, and the negative impact may be felt long after the situation is resolved. Crisis response planning is simply not optional.

As part of any plan, businesses should be proactive rather than reactive about developing a strong cybersecurity framework and information management protocol to withstand any disaster and keep the business afloat. Without proper foresight and planning, any crisis situation will place the company's reputation, brand, and profits on the line. In today's digital world, bad actors seek to take advantage of businesses struck by disaster situations, leading to the digital dissemination of misinformation, the theft of confidential or proprietary information, the intentional disruption of Internet-based business channels, and other online crises.

Organizations need to plan for a crisis before it strikes, and be ready to act quickly and efficiently when it does. Items for consideration include:

Corporate Culture of Security

The first step in any successful plan is to embrace security and integrate it with the corporate culture. Cybersecurity is not something that only the chief information officer and the chief information security officer should be thinking about. Instead, the company should select and notify specific individuals at each level who will be responsible for security well ahead of any crisis. This not only helps any company implement its plan seamlessly, but also empowers employees to recognize vulnerabilities and to speak up about them. Employees are any business' most valuable asset. A successful plan recognizes that and ensures that they are part of the solution.

It is critical to include information technology (IT) staff in emergency preparations, authorizing and empowering them to immediately respond to inquiries, both internal and external, in case of emergencies.

As many businesses have discovered during the pandemic, not all employees have remote-access capabilities. The ability to quickly pivot to remote working and maintain a remote workforce has been critical to the survival of many businesses during the still looming global crisis. Businesses that fail to adapt tend to fail.

To ensure that a business can not only survive but thrive, it must keep all staff informed of changes made to the network or infrastructure in preparing for an emergency. That makes it easier for staff to respond swiftly and efficiently without dangerous downtime when an emergency situation occurs. Training IT staff as well as network users about contingency plans and steps to be taken in case of emergency is equally important.

Wherever possible, create geographical spread and redundancy for IT staff that need to perform critical items. For example, if the IT director is unable to get to the office in South Florida because of a hurricane or a stay-at-home order, having someone on hand in Chicago who can be called on for critical tasks could be the difference between a business' success or failure.

Implement a chain of command that can be tested and kept up to date. Ensure that management communicates this information and structure to all employees. And of course, have a backup plan in case one or more employees are unavailable following a disaster incident.

Assess Business-Specific Risks

Just as not all businesses are the same, neither are cybersecurity risks. In order to comprehend cybersecurity risks faced by a particular business, the purposes for which the business collects and uses information must be considered along with the transmission, storage, and destruction of electronic data. There is no reason for any business to collect personally identifiable information (PII) that the business does not actually need. Likewise, there is no need to retain PII that the business no longer needs.

Consider the PII that a business must use as part of its operations, and utilize appropriate encryption methods (both when data is in transit and at rest) as necessary to protect that information while ensuring the company's operations run smoothly and efficiently. Consider encrypting all electronic devices or other locations where data is stored, irrespective of whether the PII at issue is sensitive or not. A pandemic or natural disaster is an unfortunate situation, but it is never an excuse to mishandle data. As business risks and needs change, management should be reviewing, analyzing, and recommending changes to risk management and crisis response protocols and processes. Crisis management should never be static, it should be reviewed and updated regularly.

Implement Limitations but Ensure That Essential Employees Can Access Critical Locations

Limit administrative rights to critical individuals who need to have such access in the ordinary course of business. This ensures that the business' security remains updated and that the business can quickly address any vulnerabilities that may arise. Company policies should require that access passwords are complex, changed often, and paired with two-factor authentication—often written as 2FA.

While security limitations are important, any emergency plan should implement access-control measures and restrictions that balance security with accessibility. This ensures that essential employees will be able to access all critical information and locations during a crisis. For example, a power failure following a natural disaster means that computer networks likely will be offline, at least temporarily. Planning for this type of disruption will mitigate the business' downtime. Be sure to advise all employees of the proper protocol in any

emergency or crisis situation, whether they play a critical role or not. Good crisis communication is imperative and includes both internal and external communications.

Out of Site and On the Mind

To ensure that a business can handle a crisis, employees should be knowledgeable about the organization's cyber infrastructure and, in particular, the requirements for key tasks and equipment location. The crisis response and emergency plan should include running a full back up on all network servers and testing to ensure that reinstallation is possible. Utilize off-site storage for all items necessary to perform reinstallations, including copies of backups, license keys, serial numbers, and configuration files.

Consider using off-site backup for all data at a data center (or multiple centers) located in areas rarely hit by natural disasters like hurricanes, tornadoes, earthquakes, or floods. Also keep in mind the possibility of other disaster scenarios such as civil unrest, riots, or terrorism. While offsite backup is not foolproof, it is an excellent business practice that has proven to protect against a wide range of disasters, including ransomware attacks. Using cloud technology to create online backups of machines can enable businesses to get employees working quickly following disruptions associated with any disaster, irrespective of where, when, or how the crisis takes place.

If the disaster event has damaged the business' physical location or if the location remains closed due to the circumstances of the disaster, consider that on-site employees may be able to effectively work remotely during a temporary period. In this situation, be prepared to issue additional corporate computing devices and accessories (e.g., headsets, webcams) for employees to use during that time. Ensure that you craft and implement meaningful policies for remote employees—whether permanent or temporary—to ensure the remote workforce is well-trained, well-equipped, and well-positioned to efficiently and effectively carry out their job duties.

The use of personal devices necessarily increases risk to the company, so always remain mindful about the business' remote workforce and ensure they not only have access to the computer network, but that they can connect securely. Remote workers may not be seen, but should not be forgotten.

Redundancy is Good, Redundancy is Good

Redundancies should be built into the infrastructure to ensure network availability and decrease the risk of failure throughout the systems. For example, alternative power sources should be available and operational, and they should be tested along with the other key components of the emergency plan, specifically those relating to equipment failure.

Remember that it is always better to be over-prepared. Businesses should invest in backup equipment to ensure a surplus. Store these items in locations that are easily accessible and preferably off-site. Remember that power outages often follow disaster incidents, so consider investing in batteries and solar-powered chargers.

The entire emergency plan should be tested regularly. Testing the portions of the plan relating to equipment failure and disruption of power are critical to make certain the technology functions properly.

Keep Employees Close and Service Providers Closer

As service providers are undeniably a crucial component of any successful business, they must be carefully vetted at the outset of any business relationship to ensure their processes conform to the business' security and privacy standards. The scope of services for any service provider should include the corporate security framework and a description of the applicable security practices. In addition to vetting, monitoring of service providers is key to ensuring they continue to comply with the appropriate standards throughout their time acting as a service provider for the business. It is the business' obligation to ensure security and privacy related compliance,

so businesses cannot and should not rely on the representations of any third party.

Businesses may be able to contract with a vendor to receive replacement hardware and software on a priority basis in case of equipment failure in an emergency. Specific possibilities should be discussed with vendors when appropriate for business needs.

Make a List and Check It More Than Twice

Crisis response and continuity plans should be kept up to date and made available to all employees so they know how to access the corporate network following a crisis situation. The plans should include a list of all critical information needed in an emergency. Keep this list on hand and keep it accurate. This list is a critical part of any emergency plan and will help protect the company's technology and business operations.

Compiling an inventory of the company's hardware and software assets and updating that list frequently seems like a daunting task. But this exercise is less daunting than attempting to create that list after a disaster while trying to rebuild and replace technology to ensure business continuity.

This critical information list should include information about all hardware and software: makes; models; operating systems; serial numbers; network devices; license keys; configuration settings; restoration instructions; support contact information; and emergency business contacts, including those for employees and vendors. Do not forget to include a list of all employees and independent contractors and their contact information so you can ensure all communications are delivered and received.

If the company does falls victim to a ransomware attack—where a threat actor gains access to and places malware on the computer system, network, or server—the threat actor will encrypt some or all files and demand a fee to return the system to normal operations. If the business is not able to pay the fee—because it cannot acquire the proper amount of Bitcoin or because the U.S. Department of the Treasury's **Office of Foreign Assets Control (OFAC) guidance** prohibits the company from making payment to the threat actor, that list may be the key to facilitating a swift recovery.

The business should also include all insurance policy information in its critical information list so that an insurance claim can be filed timely in the wake of a disaster.

Before a crisis hits, engage counsel to conduct an insurance policy review to ensure the company has adequate insurance coverage—the type of recommended coverage varies depending on a number of factors, including business type, industry, and geographic location. And if a crisis is already at your door, counsel can review the insurance policies in place to identify any potential coverage for the situation at hand.

All critical information should be saved in hard copy, but cloud storage should also be utilized to save a backup copy. With careful preparation, businesses can abate data loss in the wake of any crisis.

Cybersecurity is an evolving field with a landscape that is constantly changing. A pandemic or natural disaster creates the perfect opportunity for cyber criminals to initiate an attack on a business, a group of businesses, or even an entire industry.

Cyber Attacks on the Rise

In March 2021, the FBI released its **Internet Crime Complaint Center (IC3) 2020 Internet Crime Report**. The FBI reported that in 2020, the cost of cybercrime to individuals and businesses in the United States was approximately US$4.2 billion. This represents a 69% increase from 2019. Business email compromise scams continued to be the costliest threat (US$1.8 billion), but the majority of complaints to IC3 were about phishing scams (US$54 million).

Along with the rise in cybercrime, we have also seen threat actors becoming more sophisticated, including the conversion of funds into cryptocurrency, making recovery significantly more difficult.

Despite the rise in costly cyberattacks and notwithstanding the increased IT security investments made in 2020 to cope with the new work from home ecosystem, according to the **IDG Research Services Insight 2021 Report**, nearly 80% of senior IT and IT security leaders believe their organizations still lack sufficient protection against cyberattacks. We did see that the C-Suite and board members are more focused on overall security and almost 70% reported commencing efforts to integrate incident response into their overall business continuity plans.

Just over half of those companies conducted a data security risk assessment last year, however, and just over a quarter expanded their IT teams despite the spike in cybercrime. Given that the United States continues to experience the highest data breach costs, averaging US$8.64 million per event, crisis planning, risk management, and incident response remain high priority.

Nearly every company and every industry is at risk of a cyberattack, including threats of distributed denial of service, data security breaches, and other technology-facilitated abuse. As the internet is boundless, addressing and mitigating cyber risk is top-of-mind among companies globally. Long before a crisis occurs, companies should be aware of cyber criminals and other bad actors who utilize these disaster situations to facilitate the perpetration of fraudulent and other criminal activities. By maintaining crisis response and emergency preparedness plans that include cybersecurity and information management, businesses will be able to survive and thrive. Proper planning, including both internal and external communication planning, will help businesses mitigate risk of loss, shield profit centers, safeguard intellectual property and other critical business assets, and ensure business continuity.

The first step toward properly preparing for a crisis is for a business to take a long, hard look at its current policies and protocols to assess what a disruption would mean for business operations and what the company must improve upon in order to try and prevent or mitigate disastrous consequences. Best practices dictate that the development of an information management and crisis response plan, a comprehensive evaluation of business operations, and implementation of specifically tailored plans with proper training and implementation are the key to maximizing protection against cyber risk and information management disruption so that a business can survive any crisis.

Once a crisis passes, and when it is feasible, the business should spend time evaluating whether the implementation of the crisis response plan was a success. Revise and improve the plan and related protocols as needed to ensure that the business remains prepared to address any future crisis head-on.

ENVIRONMENTAL

Prolonged widespread emergency events, like natural disasters, pandemics, and the widespread loss of power in Texas during the winter storm event of 2021 pose a significant risk with respect to environmental compliance, particularly in circumstances where the event may hamper the ability to comply with environmental obligations. Given the complexity of state and federal requirements relating to compliance with environmental obligations during such an event, and the individual circumstances that each event poses to different regulated entities, it is important to be prepared; to understand compliance requirements before, during, and after the event; and to consult a qualified lawyer to determine the appropriate course of action. Discussed below are some considerations related to the preparation for widespread emergency events and coping with any impacts resulting therefrom.

Preparation

Different events can pose different environmental compliance and liability issues for different industries. It is important to understand the risks your specific industry and operations face in a widespread emergency event. For example, if your key personnel or vendors are curtailed during a pandemic due to stay-at-home orders or travel restrictions, environmental monitoring, analysis, and reporting may suffer. If your organization operates underground or aboveground storage tanks, flooding may damage or displace the tanks, causing discharges or releases of their contents into the environment. This in turn may cause soil, surface water, and groundwater contamination, which could result in costly environmental liability. Ensuring compliance with applicable environmental laws and regulations before an event strikes can minimize these risks.

Often, in preparing for, during, or as a result of a natural disaster, facilities must shut down operations. During shutdown, normally automated systems or process controls may be bypassed, disconnected, or operated under manual control. Of particular concern are the hazards associated with additional human interactions, as process parameters may be in unusual ranges and operators may have less experience controlling plant conditions manually. Various laws and regulations have particular requirements related to process shutdown operations, including requirements to minimize chemical releases during process shutdown operations and to report releases immediately upon constructive knowledge of the occurrence of the release. For example, facilities subject to the national emissions standards for hazardous air pollutants are required at all times to operate and maintain any affected source in a manner consistent with safety and good air pollution control practices for minimizing emissions of hazardous air pollutants, including during periods of shutdown and malfunction.[1] These concerns can persist through the reinitiation of operations, as facility startups can also trigger noncompliance issues if not properly performed.

Natural disasters may cause releases of substances not normally at issue for an organization. In some cases, these releases must be reported *immediately* to applicable authorities. As such, it is important to know in advance any reporting requirements

1 40 C.F.R. § 63.6(e)(1)(i).

that may be triggered by a release resulting from a natural disaster. For example, Section 304 of the Emergency Planning and Community Right-to-Know Act (EPCRA) requires owners and operators to immediately notify both their respective State Emergency Response Commissions and Local Emergency Planning Commissions in the event of a release of a reportable quantity of a Comprehensive Environmental Response, Compensation, and Liability Act hazardous substance or an EPCRA extremely hazardous substance.

Suspension of Rules

Many states have authority to suspend rules regarding pollution control equipment and operations at industrial and other facilities to the extent they hamper or impede responses to natural disasters. These suspensions can include, among other things, various air emission restrictions and effluent restrictions, as well as reporting, operation, maintenance, and other standards infeasible to perform during weather-related disruptions and flooding conditions. The suspensions can also include spill reporting and response requirements, 90-day limits on the storage of hazardous waste, and limits on the types and quantities of materials that can be sent to regulated landfills.

For example, during Hurricanes Harvey and Irma in 2017, both Texas and Florida implemented rule suspensions. In Texas, Governor Abbott suspended numerous rules regarding pollution control equipment and operations at industrial and other facilities to the extent they hampered or impeded responses to Harvey.[2] In addition, the Texas Commission on Environmental Quality (TCEQ) Executive Director issued regulatory guidance stating that no additional approval from TCEQ was necessary for restoration and other recovery activities directly related to the disaster.[3] Similarly, the governor of Florida has broad authority to suspend the provisions of any regulatory statute prescribing the procedures for conduct of state business or the orders or rules of any state agency if strict compliance with the provisions of any such statute, order, or rule would in any way prevent, hinder, or delay necessary action in coping with the emergency.[4] Following Irma, Governor Rick Scott authorized each state agency to determine what, if any, regulatory statutes should be suspended in accordance with Section 252.36 of the Florida Statutes.[5]

2 *See* https://www.tceq.texas.gov/assets/public/response/hurricanes/Governor-response-to-suspension-of-rules.pdf; https://www.tceq.texas.gov/assets/public/response/hurricanes/suspension-of-tceq-rules-8.28.17.pdf.

3 *See* https://www.tceq.texas.gov/assets/public/response/hurricanes/hurricane-regulatory-guidance-Harvey.pdf.

4 F.S.A. § 252.36; *see also* F.S.A. §§ 120.569(2)(n), 252.46.

5 *See* Executive Order Number 17-235.

Given the potential impact of such suspensions, it is critical that any potentially impacted party review the list of suspended rules and the stated basis for suspension at the time of the significant weather event. Generally, the suspension is only to the extent that normal operations are impossible or unsafe due to the conditions and compliance would actually prevent, hinder, or delay necessary action in coping with the disaster. In addition, regulated entities are frequently required to prepare and maintain records related to the actions and suspended rules. Please note that some state rules may have federal counterparts in statute or regulation, and suspension may not apply to such federal counterparts.

Enforcement Discretion

In addition to outright suspension of rules, environmental agencies may decide to exercise enforcement discretion if a widespread emergency event appears to make compliance problematic. A good example of what can be expected in this situation is the Environmental Protection Agency's (EPA) COVID-19 Pandemic Enforcement Discretion Memorandum.[6] In this memo, the EPA announced it would only use enforcement discretion for noncompliance that could be demonstrated to have been caused by the pandemic (e.g., key personnel shortages leading to inability to properly sample and analyze environmental emissions in a timely manner). To exercise its enforcement discretion, the EPA required facility owners to undertake reasonably practicable compliance efforts, minimize the noncompliance, and document these efforts. Among other things, the EPA applied enforcement discretion to routine monitoring and reporting required by rule, permit, and administrative settlement agreements. The EPA also applied enforcement discretion to certain noncompliance with air, wastewater, and hazardous waste emissions limits. Note, however, that the EPA did not agree to exercise enforcement discretion to noncompliance with release of reporting requirements. In the event of a widespread emergency event, facility owners and operators should check with both the EPA and their individual state agencies to determine the requirements for enforcement discretion.

The Act of God Defense

In the event that a widespread emergency event does cause potential liability, certain federal laws and state statues allow a general "Act of God" defense to liability. For example, federal Superfund law[7] (and state equivalent statutes) imposes cleanup liability on owners and operators of facilities for releases that occur at or from their facilities. The Act of God defense can relieve an owner or operator of liability if the owner or operator of the facility can demonstrate through a preponderance of evidence that the release or threatened release was caused solely by, among other things, an Act of God, as defined in the federal Superfund statute. Many statutes do not define Act of God, but as an example, the federal Superfund law defines it to be "an unanticipated grave natural disaster or other natural phenomenon of an exceptional, inevitable, and irresistible character, the effects of which could not have been prevented or avoided by the exercise of due care or foresight.[8] Additional federal statutes with an Act of God defense or compliance exemption include:"

- Oil Pollution Act, which includes an Act of God defense.[9]
- Resource Conservation and Recovery Act, which provides that the EPA may issue temporary emergency permits to permitted or nonpermitted facilities to allow treatment, storage, or disposal of hazardous wastes

6 *See* https://www.epa.gov/sites/production/files/2020-06/documents/covid19addendumontermination.pdf

7 *See* 42 U.S.C. § 9607(a).

8 33 U.S.C. § 2703(a).

9 33 U.S.C. § 2703(a).

where there is imminent and substantial endangerment to human health or the environment.[10]

- Clean Air Act, which provides for:
  - Emission restrictions for fuel-burning stationary sources during national or regional energy emergencies.[11]
  - National emission standards for hazardous air pollutants from stationary sources when in the interests of national security.[12]
  - Fuel additive requirements during natural disasters that cause extreme or unusual fuel and fuel additive supply circumstances.[13]
  - Transportation conformity requirements during emergencies or natural disasters.[14]
- Clean Water Act
  - An Act of God exception. 33 U.S.C. § 1321(f).
  - Compliance may be excused during an upset, which means "an exceptional incident in which there is unintentional and temporary noncompliance with technology based permit effluent limitations because of factors beyond the reasonable control of the permittee." 40 C.F.R. § 122.41(n)(1).
  - Exigent circumstances regarding discharges of oil and hazardous substances do not require permits. 33 U.S.C. § 1321(c); 40 C.F.R. § 122.3(d).
- Coastal Zone Management Act
  - Allows the president to authorize federal actions that are inconsistent with state coastal plans if the president finds it is in the paramount interest of the country, or the secretary of commerce determines it is a matter of national security. 16 U.S.C. § 1456(c).

Generally, in order to employ the Act of God defense or a related compliance exemption, the entity pleading the defense has the burden of proving that the alleged violation was the sole result of an Act of God, and not the result of poor planning.[15] For example, in the aftermath of Katrina, the EPA questioned the assertion of this defense and asked owners and operators to demonstrate that they had taken all reasonable steps to secure their facilities against hurricane impacts.

In the event of a significant weather event, affected parties should document any actual or threatened releases in a manner that will (a) provide evidence that supports the Act of God defense if the issue is raised later, and (b) meet any relevant state obligations that arise in the context of asserting the Act of God defense. For example, this defense is not available under Texas law to an owner or operator who subsequently transfers the facility to a new owner or operator without disclosing its knowledge about the actual or threatened release.[16] Regulated entities should keep records of all activities that they believe are covered by this defense. In some states, entities must take all necessary steps to prevent or minimize any increased risk to human health and safety and to the environment and must at all times apply best engineering and pollution control practices as required by applicable standards. As a result, regulated entities should follow their standard operating procedures, as well as startup, shutdown, and maintenance activities, requirements, and plans, to the extent feasible, even during emergency events.

10 40 C.F.R. § 270.61(a).

11 42 U.S.C. § 7410(f).

12 *Id.* § 7412(i)(4).

13 *Id.* § 7545(c)(4)(C).

14 40 C.F.R. § 51.853(d).

15 *Id.*

16 THSC § 361.275(g); TWC § 7.253(e).

INSURANCE COVERAGE CONSIDERATIONS

Natural disasters have the potential to damage entire communities and they indiscriminately affect individuals and businesses alike. The damage caused by extreme weather events is often measured in terms of collective losses exceeding US$1 billion. Hurricane Harvey, for example, judged to be one of the most costly natural disasters, yielded US$19 billion in insurance claims, and the Texas winter ice storm of 2021 has the potential to exceed that.

The losses that can arise out of extreme weather events include damage to buildings and personal property, interruption of business operations, impeded access to property, the loss of power, and other public utility services and extra expenses to resume normal business operations.

It is important that businesses impacted by severe weather events understand their insurance resources and take steps to protect and maximize their insurance recovery in the event they make a claim. Each event is likely to give rise to a variety of individualized losses, which will vary depending upon each insured business's particular circumstances. The following checklist provides a general overview of selected issues that may be relevant to the preservation and pursuit of insurance coverage for those losses.

Identifying Possible Coverage

The most common source of insurance coverage for businesses facing losses resulting from natural disasters will be the commercial property insurance policy that insures the assets of the business. Although insurers issue such coverage under a variety of standard insurance industry policy forms, some insurers have issued tailored policies to meet a policyholder's particular risk scenarios. Evaluation of the specific wording of the policy, as well as the law applicable to its interpretation, is critical.

Businesses may have first-party coverage that includes the following specific elements:

- Property damage coverage applies to damage to, or destruction of, any insured property resulting from an insured peril.

Insured property is typically defined to include buildings and other structures, equipment, supplies, and other business personal property. Most of the damage typically resulting from extreme weather events, such as water damage, wind damage and collapsed buildings, would fit under this coverage.

- Business interruption coverage generally covers the policyholder's loss of earnings or revenue resulting from property damage or loss caused by an insured peril. Accessing this coverage can present challenges, however, as the proper quantification of a business interruption loss sometimes leads to disputes.
- Contingent business interruption coverage generally covers the policyholder for losses, including lost earnings or revenue, resulting from damage to property of a supplier, customer, or some other business partner or entity that leads to that supplier or customer being unable to provide its goods/services to the policyholder or being unable to take the policyholder's goods/services. Notably, this coverage typically is written to apply even where the policyholder's own property has not been damaged.
- Attraction property coverage, which is a sub-category of contingent business interruption coverage, may apply where an insured business—such as a hotel or restaurant—suffers loss of income as a result of damage to a designated "attraction property," such as a nearby sports venue, tourist attraction, university, or convention center.
- Extra expense coverage generally covers the policyholder for certain extra expenses that it incurs as a result of a loss event in order to resume normal operations to the extent possible or to mitigate other losses.
- Ingress and egress coverage generally covers the policyholder for economic losses when access to a business premises or location is prevented for a time, e.g., if the access roadway leading to the policyholder's business has collapsed.
- Civil authority coverage generally covers the policyholder for economic losses arising from an order of a governmental authority that interferes with normal business operations. Similar to contingent business interruption coverage, civil authority coverage may apply even when there is no damage to the policyholder's own property.
- Service interruption coverage generally covers the policyholder for economic losses related to electric or other power supply interruption. Often this coverage is written to require the outage to be the result of a damage event to the utility provider's equipment within a certain distance of the policyholder's property.
- Advance payments by the insurer may be expressly required under the terms of a commercial property policy, even if the full extent of the insured loss is still being investigated and adjusted. Such advance payments can be important where a business cannot afford a protracted adjustment period before receiving funds for repairs and to replace a lost stream of income.
- Claim preparation coverage generally covers the policyholder for the costs associated with compiling, supporting and certifying a claim for coverage.

Presenting a Claim

Most policies include specific procedures describing how and when a claim must be presented and documented. Some of these procedures may have timing deadlines associated with them. Failure to timely comply with these procedures may give insurers a basis to attempt to deny an otherwise covered claim.

In addition, the manner in which a claim is presented by the policyholder to its insurer can have a significant impact on the ultimate recovery,

particularly in the context of applying limits of liability and determining which deductibles or self-insured retentions apply. As a result, policyholders should be proactive in assembling an insurance recovery team, including working with accountants and claim professionals as well as insurance coverage counsel. At a minimum, a policyholder should consider the following common, potentially time-sensitive policy provisions:

- Notice of Loss. Most policies require the policyholder to provide notice "as soon as practicable" or within a specified time period after learning of a claim, or sometimes even after learning of circumstances that may lead to a claim. Policyholders should be mindful of such deadlines and also should carefully evaluate whether they may have rights as an insured not only under the policy purchased directly by them, but also under some other policy. For example, a property owner may have rights to insurance coverage (as an additional insured) under the policy issued to a business leasing space and operating on the property.
- Proof of Loss. Property policies generally require that a policyholder submit a sworn "proof of loss" summarizing the amount and extent of the damage or loss. The policy language may purport to require this proof of loss be submitted within a specified timeframe (e.g., 60 or 90 days), though it is not uncommon for insurers to agree to extend this deadline, if so requested. A policyholder should consider requesting a written agreement extending the time for submission of a proof of loss (and potentially other policy conditions) depending on the nature and complexity of the loss. Additionally, insurers may require that the policyholder provide extensive detail in support of its claim. Accordingly, policyholders should assemble and maintain all relevant documentation that may support their claim, including making a photographic or video record of damage to buildings, equipment, materials, and inventory; keeping copies of estimates, invoices, and receipts for any repairs or other covered losses/costs; and maintaining comprehensive and detailed financial records to support any business interruption or contingent business interruption claim.
- Suit Limitation. Policies often include a "suit limitation" provision, which provides that an action to recover under the policy is barred if not initiated within a certain timeframe (e.g., "within 12 months of the loss"). In some states, these provisions may not be enforceable if they provide for a period less than a statutory limitations period or other minimum amount of time, while in other states, they are enforceable. Businesses should consult counsel to determine what limitations period may be applicable to the pursuit of their claim in litigation.

Common Insurer Responses

In light of the large number of claims that typically result from natural disasters, and the tremendous overall value of those claims, insurers can be expected to raise a number of potential limitations or restrictions on coverage when presented with a claim. Here are just a few of the common issues that may be raised by insurers:

- There was no covered business interruption. Insurers often take a narrow view of what constitutes a business interruption, sometimes arguing that a complete cessation of operations is necessary to support a claim. The insurer may also dispute the necessity or cause of the interruption. For example, the insurer may argue that at least some part of the interruption or reduction in an insured business was the result of an unrelated business decision by the policyholder, or the consequence of an economic downturn, and it was not caused solely by damage to insured property as the result of the natural disaster.

- The claim involves multiple 'occurrences' under the policy, each of which is subject to a separate per-occurrence deductible. Most policies have a per-occurrence deductible or other self-insurance feature that may reduce the amount of coverage available, depending on how the number of occurrences issue is addressed. In particular, there may be disputes about whether the entirety of a business's loss was the result of a single natural disaster, or instead involved multiple weather patterns or cycles that constitute multiple occurrences under the policy.
- Some of the property damage is of a type excluded under the policy, such as for 'flood.' Although many businesses—particularly large commercial enterprises—have "all risk" policies that explicitly include some measure of coverage for "flood," many others do not. In the aftermath of some previous natural disasters, some insurers have taken strained positions in an attempt to characterize their policyholders' water-related damage as excluded "flood"-related damage, even with respect to water damage to the interior of a building caused by a burst pipe.
- The claim is for losses beyond the allowed recovery period. Policies may include provisions specifying that they only cover loss of income and related expenses for a specified period of time after an insured event occurs. If the policy does not define that period, it may be tied to the time it would take a policyholder, employing reasonable mitigation efforts, to resume normal business operations under the circumstances. In view of the magnitude of the losses following natural disasters, the length of time it will take to repair property and resume normal business operations may be longer than the length of time had the claim been from an isolated event affecting a single facility.

Conclusion

Businesses that have suffered losses because of natural disasters should not overlook the significant financial protection that may be provided through their insurance policies. Businesses should act carefully and proactively— in advance—to protect and help maximize their coverage. Experienced insurance coverage counsel is often needed to assess the viability and strength of a policyholder's claim, in dealing with an insurer's loss adjusters, and in maximizing the policyholder's potential insurance recovery. We have represented clients in dealing with claims arising from many types of natural disasters and perils, including storms, hurricanes, wildfires, floods, as well in other complex insurance claims for over 35 years. Our team is dedicated to assisting policyholders in assessing and prosecuting insurance coverage claims.

LABOR, EMPLOYMENT, AND WORKPLACE SAFETY

Natural disasters raise a host of potential legal issues for employers operating in the affected areas. Whether the disaster strikes the business's main headquarters or a small satellite office, employers must be ready for emergency weather situations with an effective and easily implemented action plan. In addition to primary safety concerns, employers must consider the various state and federal laws implicated in emergency weather situations and assess whether continued business operations comply with such laws. Further, in 2021, employers will need to continue considering how to carry out an emergency action plan while complying with public health recommendations relating to social distancing and face coverings due to the pandemic.

In order to successfully navigate these unique employment challenges, employers should take proactive steps in advance of natural disasters to create and implement a comprehensive disaster preparedness plan that enables employers and employees to safely manage the changes that impact the workplace. In light of the pandemic, employers should be reevaluating their disaster preparedness plan to make sure it is tailored to the current status of the workplace, such as all employees working onsite or all employees working remotely.

With the guidance of legal counsel, employers should consider the following issues in developing an action plan and assessing possible strategies for handling a crisis.

Test and Communicate Disaster Preparedness Plan Yearly

Employers should implement a disaster preparedness plan and test it annually. Employers should adapt the plan from year to year to suit the needs of the business and the changes to the facilities. For example, in 2021, employers may need to adapt the plan to address social distancing concerns, including updating evacuation routes to accommodate social distancing and requiring employees to wear face coverings while evacuating. Once employers have adequately tested the disaster preparedness plan, they should communicate this plan to all employees. Employers should deputize a contact person to address any questions employees may have about the disaster preparedness plan. Even if an employer does not make changes to the disaster preparedness plan in a given year, employers should still communicate the plan annually and remind employees of its procedures. As more employees are returning to in-person work, in some cases for the first time in months, employers should take advantage of this opportunity to remind all employees of disaster preparedness procedures.

Emergency Notification System

In order to ensure effective and safe communication with employees during a natural disaster, employers should consider instituting an emergency notification system—to the extent they do not have a system already in place—that will alert employees of natural disasters or other crises. For example, employers may choose to implement a severe weather hotline, system-wide email notifications, or text message alerts to inform employees of emergency weather situations and potential office closings. Employers that choose to implement an emergency notification system should inform all employees, even those working remotely, of any anticipated office closures. Employers should confirm that their preparedness policy clearly

outlines the best form(s) of communication for employees in the event of a crisis. Employers should also verify employees' personal contact information in advance of severe weather, including phone numbers, email addresses, and emergency contact information. Depending on the size and nature of the business, employers may decide to designate certain individuals within the preparedness plan to oversee the verification process and ensure that all employees are set up for safe, effective communication.

Office Closings

While many offices continue to operate at a limited capacity during the pandemic, developing a plan to handle office closings is still a primary issue to consider when developing a disaster preparedness plan. Employers must use their discretion in determining whether an office closing is necessary, but they may consider implementing certain guidelines that standardize the protocol and provide employees with a better understanding of the company's general policy. For example, employers should determine whether the issuance of a severe weather advisory (e.g., a tropical storm or hurricane warning) or an evacuation order will trigger an automatic office closing. Similarly, employers should consider whether office closings will coincide with local government or public school closings.

Given that some employees may not reside in the same county as their workplace, employers may need to consider how to handle employees whose areas of residence are under greater threat. For instance, while the office may be located in a safe zone, some employees may live in areas for which an evacuation order has been issued and, therefore, may need to leave work early to make preparations. Employers should allow employees sufficient time to travel to their homes in a safe manner. Further, considerations should be made for employees working from home who may experience power outages or related damage in the area where they live.

Many employers need to continue operations during severe weather events. Employers should consider whether the needs of the business are such that certain employees must remain on site during the natural disaster, such as maintenance workers who handle emergency repairs or are otherwise necessary for continued operations. A disaster preparedness plan should identify essential personnel versus nonessential personnel for purposes of operating during a severe weather situation and determine whether a separate protocol is needed to govern the responsibilities and dismissal of essential personnel.

In some instances, employers may need to continue operations despite state or local governments declaring a state of emergency. Before disciplining an employee who fails to report for work during the state of emergency, employers should ensure that applicable state law does not prohibit employers from terminating or disciplining employees for failing to report during a declared state of emergency.

Compensation During a Natural Disaster

Once an employer has made the decision to close the workplace, the next issue is whether and how employees will be compensated for the duration of the closing. Specifically, employers should determine how to handle nonexempt employees versus exempt employees with respect to compensation during natural disasters, and they should articulate this policy in the disaster preparedness plan.

If the workplace is closed for a period of time that is less than a full workweek, then employers must pay an exempt employee's full salary for that week. However, employers may require exempt employees to use their available leave during severe weather closings. With respect to nonexempt employees, the Fair Labor Standards Act (FLSA) requires employers to pay nonexempt employees only for hours actually worked. As a result, an employer generally is not required to compensate nonexempt employees who are unable to work due to a natural disaster. Employers should be mindful, however, that an exception to this rule exists with respect to employees who receive fixed salaries for fluctuating workweeks; these employees are entitled to their full weekly salary for any week in which any work is performed.

To the extent an employer decides to compensate nonexempt employees who are unable to work during a severe weather closing, the disaster preparedness plan should specify the standard pay

and leave practices. For example, some employers choose to compensate nonexempt employees for a full workday where the employees report to work but are forced to leave early due to a severe weather warning. Similarly, some employers consider paying employees up to a certain number of days for office closings due to a natural disaster. Regardless of the desired arrangement, employers should confirm that their action plans include clear guidelines regarding compensation and treatment of leave during severe weather incidents and that these guidelines are applied to all similarly situated employees equally.

Employers must also consider nonexempt employees' roles with respect to continuing operations, both remotely and on site. An employer may be required to pay an employee who remains "on call" during a disaster depending on whether the employee is actually working during those hours. For example, in the case of a maintenance worker who remains on site to handle emergency repairs, the employer is required to compensate the employee for his or her "on call" hours during the disaster. Certain remote "on call" duties, however, may not constitute hours worked for purposes of the FLSA, and thus, employers should consult with legal counsel as to whether such remote employees are entitled to compensation for their "on call" time.

Further, employers should be mindful when allowing employees to "volunteer" during a severe weather emergency. An employee's voluntary assistance during a natural disaster does not constitute volunteer work for purposes of the FLSA if the employee performs the same services he or she is regularly employed to perform. Likewise, if an employer requires or mandates that employees help with pre-disaster preparations (e.g., boarding windows) or other disaster-related work, the employer must compensate the employees for any hours worked. When designating any sort of severe weather support team or requesting pre-disaster assistance, employers should keep in mind that certain employees may be entitled to compensation depending on the responsibilities assigned.

In some circumstances, employers may consider relocating particular employees to a designated remote location to ensure business continuity. In addition to ensuring proper compensation for work completed during the relocation period, employers must also consider, among other issues, whether employees will be reimbursed for travel expenses arising out of the relocation process, whether there will be any sort of fund available to the relocation administrator for petty expenses, and whether travel time will be included in hours "worked" for purposes of compensation.

Reopening the Office

Once the severe weather has subsided, employers must consider a variety of legal issues with respect to reopening office locations and resuming business operations. In the wake of a natural disaster, employees may be returning to a significantly damaged workplace in need of repairs. Above all, employers must account for employee safety. Pursuant to the standards promulgated by the Occupational Safety and Health Administration (OSHA), certain employers are required by law to provide a workplace free from serious recognized hazards and examine workplace conditions to ensure that they conform to applicable OSHA standards. Before reopening the business premises to employees after a natural disaster, employers should carry out effective procedures to inspect the property and ensure the facility is in fact safe for employees to resume operations.

Employers should also be aware, to the extent the workplace requires clean-up and repairs, of the potential risks and dangers associated with restoring the premises. For example, where a workplace has flooded and suffered significant water damage, employers should be careful assigning tasks involving electricity to untrained employees. Employers should assess the potential risks specific to their facilities (e.g., chemicals stored on the premises, layout of electrical wiring) and account for these risks in their response plan. Employers should also consult with legal counsel to ensure their

disaster response practices are OSHA-compliant and review the local and state regulations implicated with respect to any accidents or injuries to employees that occur as a result of responding to the disaster.

Employers will also need to consider potential leave issues associated with the reopening of a facility following a natural disaster. Employees are typically expected to report back to work as promptly as they are able to do so. However, to the extent an employee's area of residence is still impacted by the weather such that the employee is unable to travel safely to the workplace, employers should consider such absences as time off for "personal reasons," as suggested by the Department of Labor. Under such circumstances, an employer may consider whether to place an exempt employee on leave without pay for the full day or require the employee to use his or her accrued vacation time. Employers should confer with legal counsel before docking a salaried employee's pay.

Under certain circumstances, employees may be entitled to a reasonable accommodation under the Americans with Disabilities Act based on physical or emotional injuries as a result of the natural disaster or other crisis.

In addition to workplace damage, employees may be dealing with significant damage to their homes and vehicles. While federal law does not require employers to give employees time off to repair their homes and clear out the wreckage, employers should consider whether they want their disaster preparedness policy to provide employees with a certain amount of leave reserved for such situations. If employers choose to carve out specific leave for these circumstances, their disaster policy should clearly outline the criteria to trigger such leave and ensure that the leave is applied fairly and equally to all employees in need.

Employers should also be mindful that some employees may be entitled to leave under the Family and Medical Leave Act in the aftermath of a natural disaster. For example, an employee whose elderly parents have lost power due to a storm may be entitled to leave to care for the parents. Further, an employee who suffers from anxiety or depression as a result of the crisis may also qualify.

Employers should be aware that under the Uniformed Services Employment and Reemployment Rights Act, employees who take leave to serve in the National Guard or other similar military service during a natural disaster are entitled to reemployment after their duty is complete.

Similarly, employers with employees who serve as volunteer first responders should be aware that they may have obligations under state law to protect their volunteer first responder employees from discrimination or discharge as a result of their service.

Permanent Closings

Unfortunately, not all businesses survive the trauma of a natural disaster. In the most severe circumstances, some employers are forced to permanently close a business location as a result of the destruction or loss of business. To the extent employers must close shop or undergo significant layoffs, the Worker Adjustment and Retraining Notification Act (WARN) may be implicated. In addition, certain states have mini-WARN acts that may also be implicated. WARN, as well as these state mini-WARN acts, impose notice requirements on certain employers with respect to plant closings and mass layoffs and mandate that employers provide employees with as much notice as possible given the circumstances. In developing a disaster preparedness plan, employers should seek guidance from legal counsel to determine whether the federal or state WARN acts apply to their business and, if so, whether they have appropriate notification procedures in place.

MERGERS AND ACQUISITIONS

While typically not the first subject that comes to mind when initially approaching mergers and acquisitions (M&A) transactions, disaster preparedness and the related issues can play a crucial role in almost every stage of a contemplated M&A transaction, from diligence on the target and negotiation of the definitive agreement through closing of the deal to dealing with post-closing indemnity claims and earn-outs.

While this is true to varying degrees for all M&A, it is especially important to give proper attention to disaster preparedness issues for transactions in which one or more of the parties are located in South Florida or other parts of the state, including the Florida panhandle. Given the entire region's propensity for lightning, susceptibility to flooding in coastal areas, and annual risk of falling victim to devastating storms during hurricane season, such transactions are at a higher risk of being adversely affected by natural disasters.

This chapter provides a general overview of certain key considerations relating to disaster preparedness issues in M&A transactions, specifically those involving buyers or targets in Florida. While this discussion is focused on Florida, many of the issues and principles addressed here may also apply to other regions that are at increased risk of natural disasters.

Diligence

In preparing for due diligence on a target that is located in Florida or that has critical assets in Florida, buyer's counsel should cooperate closely with the buyer to develop an understanding of what target assets and resources are material to the buyer or critical to the ability of the target to operate

its business. Buyer's counsel should then tailor its due diligence requests and related diligence review and analysis to confirm the extent to which such assets and resources are at risk in the event of a hurricane, flooding, or other natural disaster and what disaster mitigation steps the target has implemented (or should implement) to reduce that risk. For example, a buyer evaluating a Florida target that operates nursing homes may wish to investigate the target's disaster preparedness plan, including whether it has emergency backup generators for electricity, which are imperative for such issues as ensuring temperature-sensitive medications do not spoil or residents sensitive to high heat have access to air-conditioned spaces. In this case, the buyer should determine if those backup generators are regularly maintained and properly protected against power surges and that each nursing home maintains sufficient generator fuel on site to power the generators for a reasonable time in the event of a hurricane or other disaster that results in loss of power. It may also be prudent to investigate as part of the diligence effort whether each nursing home has a reasonable, practicable evacuation plan to get residents to safety should an evacuation order be issued or if the generators fail or run out of fuel.

A due diligence process that thoughtfully engages with disaster preparedness issues will aid the parties in negotiating meaningful and appropriate risk allocation mechanisms in the definitive agreement with respect to hurricane and other natural disaster-related risks, including representations and warranties, closing conditions (for deals involving delayed signing and closing), and post-closing indemnifications or earn-outs.

While not usually thought of as due diligence in the traditional sense, the target may also wish to engage in some diligence to understand the risks that natural disasters may pose to the buyer if the buyer is located in Florida, including assessment of the likelihood that a hurricane or other natural disaster could impede the ability of the buyer to close on the transaction or to fulfill post-closing earn-out obligations.

Negotiation of Definitive Agreement and Closing

Representations and Warranties

Generally speaking, the target's representations and warranties in M&A agreements serve the dual function of forcing the seller to perform self-diligence (so as to be in a position to provide meaningful and correct disclosure against such representations and warranties) and of allowing the parties to allocate certain risks, especially to the extent that the buyer is entitled to indemnification for breaches of representations and warranties. Similar to the approach to the due diligence requests and related investigation, buyer's counsel should negotiate meaningful representations and warranties that specifically address key hurricane and other natural disaster risks to which a target is subject. In the above example of a target company that operates nursing homes in Florida, appropriate representations and warranties would confirm the disaster preparedness status of the nursing homes, including its backup generators and evacuation plans. Additionally, buyer's counsel may wish to include representations and warranties confirming that the nursing facility, in all respects, complies with or exceeds specific standards of rain and wind resistance, is equipped throughout with hurricane shutters or hurricane impact windows, and is otherwise able to withstand hurricane-force winds and conditions. As is often the case, nuance is of critical importance. The applicability of building codes usually depends on the date a building was permitted, not the date it was built. As a result, a generic representation and warranty that the nursing homes are compliant with "applicable building codes" may not be sufficient to establish that they are compliant with more recent codes established to provide greater protection against hurricane-force winds.

Closing Conditions

M&A transactions involving a delayed signing and closing customarily include a set of often

heavily negotiated conditions precedent that must be fulfilled to obligate the parties to proceed to closing. While many of these conditions relate to common legal or commercial matters (e.g., buyer can obtain the necessary financing or seller can obtain necessary third-party consents to a change of control or antitrust clearance for the merger to proceed), for M&A transactions involving either a buyer or seller who are exposed to natural disaster risks, both buyer's and seller's counsel should consider whether any special conditions would be appropriate or whether certain customary closing conditions, such as the absence of a "material adverse effect" on the target between signing and closing of the transaction, should be adjusted to specifically account for risks relating to hurricanes and other natural disasters. This allows the parties to allocate the risk of a hurricane or other natural disaster intervening between the signing and the closing. It also allows the buyer to impose conditions specifically relating to the target passing certain disaster preparedness standards. Finally, given the close interplay between closing conditions and pre-closing covenants (which are discussed below), it also allows the buyer to ensure that all pre-closing covenants are performed to the buyer's satisfaction. In the above nursing home example, the buyer may wish to negotiate that, as a condition to closing, all of the emergency generators pass a comprehensive inspection certifying them to be in full working order and that a supply of no less than some agreed number of days of generator fuel be present on site at each nursing home.

Pre-Closing Covenants

Pre-closing covenants, which are another common feature of M&A transactions with a delayed signing and closing, typically govern the conduct of the business of the target between the signing and the closing. Usually, in designing these covenants, the buyer's goal is to preserve the status of the target as closely as possible from the signing date through the closing. Here, too, it is worthwhile to consider including covenants that are specific with respect to disaster preparedness. Pre-closing covenants also offer the parties, especially the buyer, an opportunity to ensure that the seller remedy any deficiencies identified during due diligence. In the above nursing home example, if the emergency generators are in disrepair, the buyer may require the seller to covenant that all emergency generators are repaired and undergo comprehensive inspection prior to closing. Similarly, the buyer may require the seller to covenant that in the event of a hurricane, prior to closing, the seller will make all necessary preparations for the nursing homes and the residents for the hurricane and otherwise will take all reasonable steps directed by the buyer to protect the nursing homes and their residents.

Termination/Walk-Away Rights

Interplaying closely with closing conditions and pre-closing covenants, termination or walk-away rights govern when a buyer (or, though more seldom, seller) may walk from a signed M&A agreement between signing and closing. Once again, specificity when addressing disaster preparedness can be crucial in protecting the buyer's or the seller's interests. Because a termination right is sometimes seen as an extreme remedy, it is not uncommon for parties to instead negotiate purchase price adjustments (e.g., reductions) that apply if certain events occur between signing and closing rather than giving the buyer a walk-away right for those events. Reverting, once again, to the above nursing home example, while the mere occurrence of a hurricane prior to closing should arguably not let a buyer off the hook from its obligation to close, buyer's counsel would be reasonable to ask that damage in excess of some pre-negotiated threshold as a result of any hurricane or other natural disaster to the nursing homes would give the buyer the right to walk away from the transaction. Seller's counsel, on the other hand, may instead try to negotiate for the seller to have the right to fix such damage or to have the purchase price reduced for the amount of such damage. Absent sufficiently specific closing conditions, a buyer may find itself in the unenviable position of being forced to proceed to closing despite significant damage having been

suffered by the target as a result of an intervening hurricane or other natural disaster—a potentially devastating result from the buyer's perspective but a boon from the seller's perspective. Finally, a note regarding force majeure: If the M&A agreement contains a generic force majeure clause (including the typical "Act of God" or similar language) but also specifically addresses hurricanes and other specific or generic natural disaster-related risks elsewhere in the agreement, such as in the termination or walk-away rights section, then it may be advisable to insert appropriate limiting language in the force majeure clause to clarify which provision should apply in the event of a hurricane or other applicable natural disaster to avoid dispute over which provision controls the parties' rights and remedies in the event of such a natural disaster.

Post-Closing

Post-Closing Indemnity Claims

In most M&A transactions, the sellers will indemnify the buyers for, among other things, breaches of representations and warranties and, where applicable, breaches of certain pre-closing covenants not waived by the buyer. In situations where the seller does not provide indemnity and there is no escrow, the buyer may also consider availing itself of representation and warranty insurance to limit its exposure. While indemnity provisions are among the most tensely negotiated provisions of an M&A agreement, their value is inherently tied to the quality of the representations and warranties and any applicable qualifications, materiality thresholds, and baskets (or deductibles) that make recovery of indemnity either easier or harder for the buyer. The ease with which recovery for valid indemnity claims can be made also depends on the availability of funds, a reason that many buyers insist on some percentage of the purchase price being deposited into escrow for some agreed period of time to ensure that there will be (at least some) funds against which the buyer can recover if a valid indemnity claim exists. All of these mechanisms in their multitude of permutations are, ultimately, a way of allocating and shifting risk between the buyer and seller. In negotiating them, however, the parties would be remiss not to consider the special risks that apply to the transaction and the parties, including the risk of natural disasters in regions where they are more likely to occur—such as the increased risk of hurricanes (and other storms), lightning, and flooding in Florida. In the above nursing home example, the buyer may insist that the seller indemnify the buyer in the event that breaches of the representations and warranties regarding the good working condition of the emergency generators result in damages to the nursing homes or injury to the residents during a power outage caused by a hurricane or other natural disaster.

Post-Closing Earn-Outs

Transactions with a post-closing earn-out may also be affected by disaster preparedness considerations, especially with respect to (usually very highly negotiated) earn-out reductions or true-ups for pre-agreed items. For example, a seller may wish to negotiate that post-closing earn-outs will not be reduced for damages resulting from hurricanes or other natural disasters unless such damages are caused by deficiencies in the target's disaster preparedness that existed prior to closing. In the nursing home example, the buyer and seller may agree that any earn-out payments will be reduced to the extent remedial work performed by the seller to correct code violations or generator malfunctions discovered in due diligence was improperly performed and such improperly done remedial work resulted in damages to the nursing homes or their residents. In the same example, the seller may wish to carve out from the reductions any damages that result from buyer's failure to properly maintain generators that worked perfectly well prior to closing.

Most "form" M&A agreements may, directly or indirectly, cover many of the above topics. It nevertheless behooves the buyer and seller and their respective counsels to carefully evaluate whether, where, and how to specifically and

expressly address disaster preparedness issues, rather than relying on boilerplate, when dealing with M&A transactions that involve parties or assets in Florida given the greater risk of certain types of natural disasters in that region. While it may sometimes be a strategic decision by a buyer or seller to leave the M&A agreement or specific provisions of it silent on disaster preparedness issues, to make such a strategic decision requires those issues to first be identified and analyzed.

K&L GATES

K&L Gates is a fully integrated global law firm with lawyers located across five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants, and entrepreneurs in every major industry group, as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit klgates.com.

22242