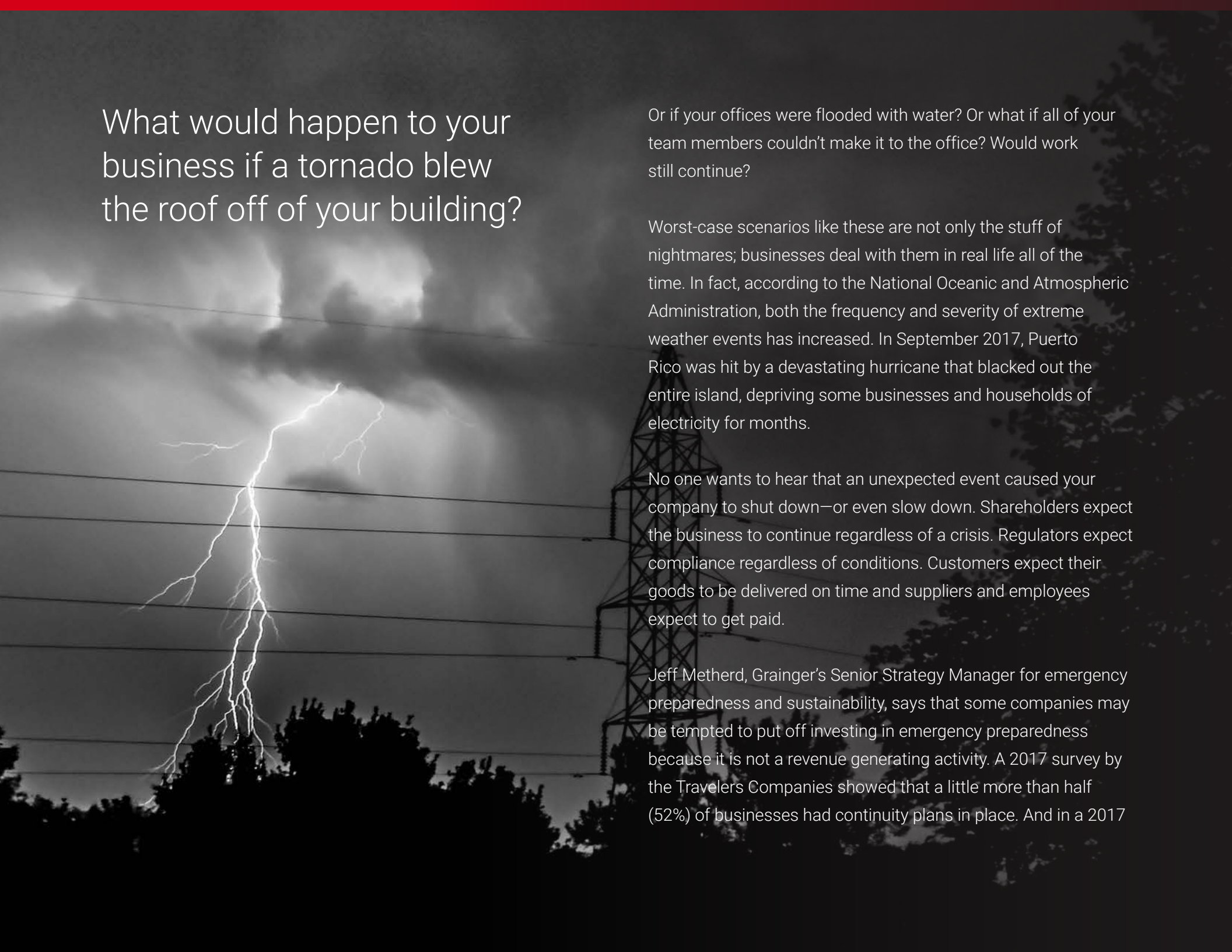
YOUR TEAM'S GUIDE TO EMERGENCY PREPAREDNESS, BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

GRAINGER



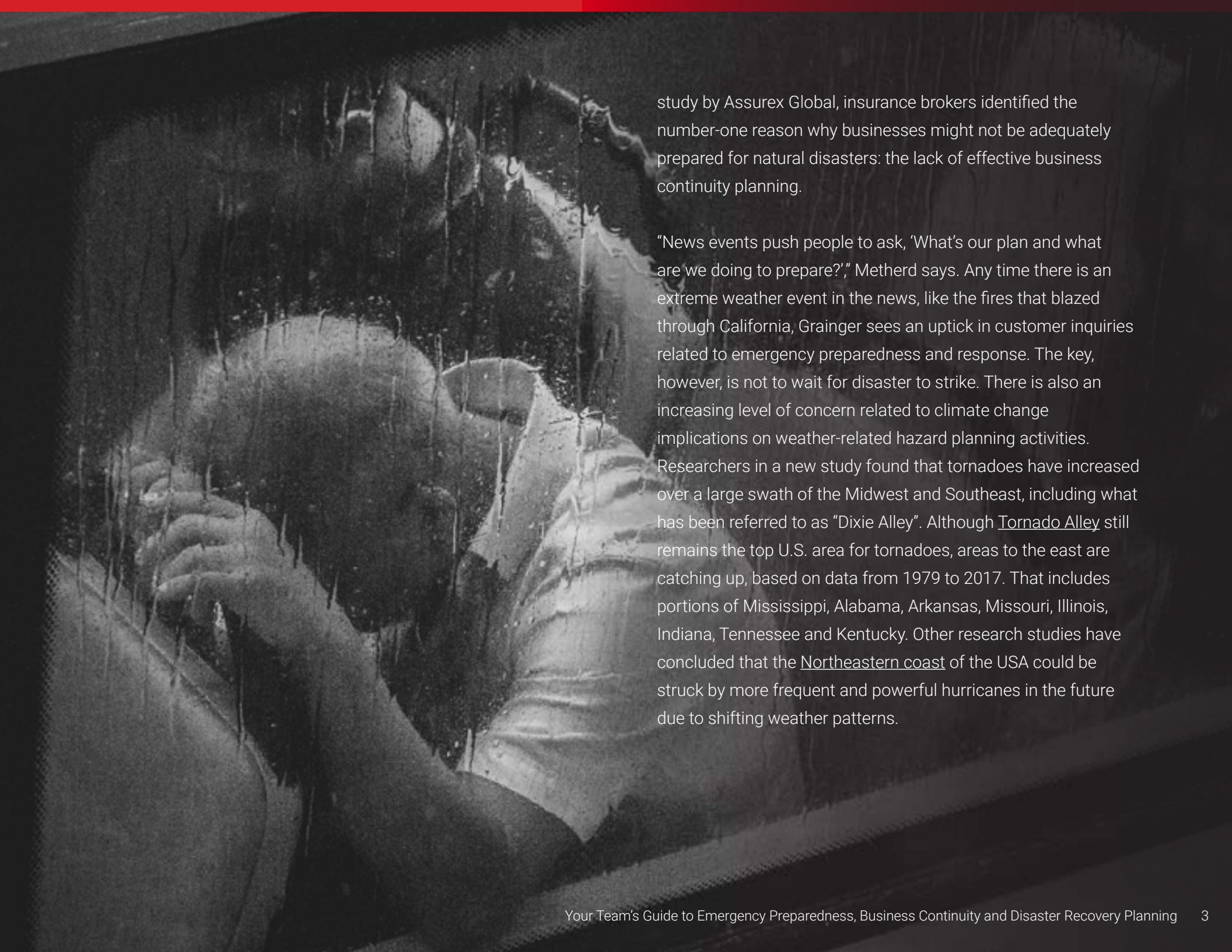
What would happen to your business if a tornado blew the roof off of your building?

Or if your offices were flooded with water? Or what if all of your team members couldn't make it to the office? Would work still continue?

Worst-case scenarios like these are not only the stuff of nightmares; businesses deal with them in real life all of the time. In fact, according to the National Oceanic and Atmospheric Administration, both the frequency and severity of extreme weather events has increased. In September 2017, Puerto Rico was hit by a devastating hurricane that blacked out the entire island, depriving some businesses and households of electricity for months.

No one wants to hear that an unexpected event caused your company to shut down—or even slow down. Shareholders expect the business to continue regardless of a crisis. Regulators expect compliance regardless of conditions. Customers expect their goods to be delivered on time and suppliers and employees expect to get paid.

Jeff Metherd, Grainger's Senior Strategy Manager for emergency preparedness and sustainability, says that some companies may be tempted to put off investing in emergency preparedness because it is not a revenue generating activity. A 2017 survey by the Travelers Companies showed that a little more than half (52%) of businesses had continuity plans in place. And in a 2017



study by Assurex Global, insurance brokers identified the number-one reason why businesses might not be adequately prepared for natural disasters: the lack of effective business continuity planning.

"News events push people to ask, 'What's our plan and what are we doing to prepare?'," Metherd says. Any time there is an extreme weather event in the news, like the fires that blazed through California, Grainger sees an uptick in customer inquiries related to emergency preparedness and response. The key, however, is not to wait for disaster to strike. There is also an increasing level of concern related to climate change implications on weather-related hazard planning activities. Researchers in a new study found that tornadoes have increased over a large swath of the Midwest and Southeast, including what has been referred to as "Dixie Alley". Although Tornado Alley still remains the top U.S. area for tornadoes, areas to the east are catching up, based on data from 1979 to 2017. That includes portions of Mississippi, Alabama, Arkansas, Missouri, Illinois, Indiana, Tennessee and Kentucky. Other research studies have concluded that the Northeastern coast of the USA could be struck by more frequent and powerful hurricanes in the future due to shifting weather patterns.

This eBook focuses on making sure your organization has the tools to prepare for a potential disaster, and provides information that business leaders can utilize to help prepare for the hazards their organization may face.

TABLE OF CONTENTS

THERE ARE FOUR PHASES OF EMERGENCY PREPAREDNESS:

1. Mitigation
2. Preparedness
3. Response
4. Recovery

Mitigation focuses on preventing future emergencies and minimizing the effects of those emergencies.

Preparedness is all about designing plans to mitigate impact, save lives, and enabling response and rescue operations before disaster strikes.

Response includes knowing how to react to all of the activities taking place during an emergency and responding safely.

Lastly, the **recovery** phase includes actions you can take to return to a state of normal or an even safer state than before the emergency took place.

Every facility faces unique potential threats depending on where they are located. If you're located in Iowa, for example, you will most likely need to prepare for tornadoes but not necessarily hurricanes. According to the Department of Homeland Security, in developing an all hazards preparedness plan, potential hazards should be identified, vulnerabilities assessed and potential impacts analyzed.

When performing a risk assessment, companies should assemble a cross-functional team and ask, "What are the hazards that are most likely to occur?" A vulnerability assessment involves answering the question, "What are the assets at risk?" Finally, a business impact analysis examines how property damage, casualties or business interruption would impact the company's ability to operate. Guidance on conducting risk assessments, hazard identification and business impact analysis can be found at ready.gov/planning, as well as the Ready Business Toolkits. These toolkits include hazard-specific versions for earthquake, hurricane, inland flooding, power outage, and severe wind/tornado.

Implementing a preparedness plan also involves identifying and assessing resources which may include people, facilities equipment and supplies. The availability of resources often depends on logistics— the management of resources to get them to where they are needed when they are needed.

Grainger helps both public and private sector organizations identify and procure critical supplies and equipment before emergencies happen so that in the event of a crisis, they have the capability to respond. Based upon the most critical hazards and vulnerabilities identified, a Grainger representative can then identify hazard-specific supplies and equipment that may be required before, during and after emergency events occur.

When a disaster occurs or is imminent, Grainger's Corporate Emergency Response Team assembles to decide if and when to activate support. If it is a large-scale event with the potential to significantly impact Grainger's supply chain, this cross-functional team assembles for ongoing conference calls. The team discusses potential disruptions to transportation networks, inventory levels for critical items expected to be in high demand and the expedited transport of critical items to the affected area within Grainger's nationwide supply chain network if an emergency were to occur. Grainger then shares the information with customers so they know what critical supplies are in stock and available.

The goal of Grainger's coordinated efforts, according to Metherd, is to engage with its customers early in the process. By creating your emergency preparedness plan early, it's easier to see the link between emergency preparedness and business continuity: With a robust emergency preparedness plan, companies can better develop the capability to operate normally following an emergency.

The terms **"business continuity"** and **"disaster recovery"** are often used together, to the point where many companies use them interchangeably. That's not entirely a bad thing: while there are important differences, the people, places and processes involved in business continuity and disaster recovery should be aligned in order to work as they should.

BC

BUSINESS CONTINUITY PLANNING
refers to a strategy that allows a company to operate with minimal downtime in the face of a catastrophic event.

DR

DISASTER RECOVERY PLANNING
on the other hand, means developing the capabilities necessary to restore the data and applications that support businesses in case of downtime.

It's not hard to see why the two should go hand in hand and why difficulties might ensue if they don't.

Business continuity and disaster recovery often have the word "planning" associated with them. While planning is important, it represents only the beginning of a process that needs to include testing, training and execution. Too many companies fail to grasp that having a plan on the shelf doesn't mean that the business is prepared to handle a critical event.

1

Writing the Plan

There are plenty of public resources to draw on in developing a suitable plan. The International Organization for Standardization (ISO) that provides standards for business continuity and disaster recovery are the most widely used globally, and are gaining acceptance in the United States. One standard, ISO 22301:2012, provides a foundation for developing business continuity management systems and auditing BC programs. ISO 22313:2012 provides a how-to guide to support 22301's requirements.

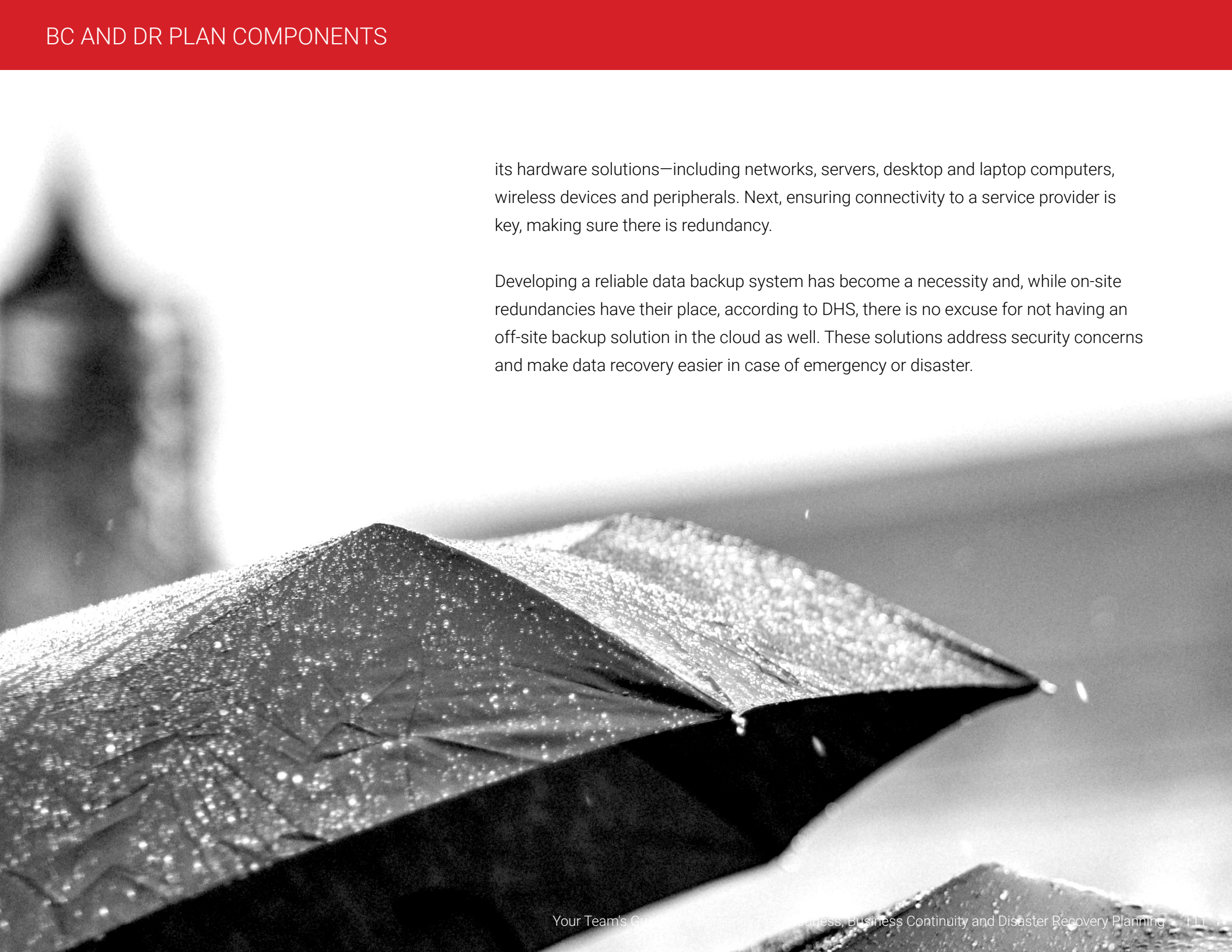
The U.S. Federal Emergency Management Agency (FEMA) has published a widely-used guide to BC and DR planning and execution. It's called "Emergency Management Guide for Business and Industry: A step-by-step approach to emergency planning, response and recovery for companies of all sizes."

The U.S. Department of Homeland Security (DHS) also has helpful BC and DR guidelines at ready.gov/business. DHS suggests that organizations take a comprehensive approach to tackling disaster recovery by factoring hardware, software, data and connectivity into their plans.

To ensure that all critical systems are addressed, DHS recommends that organizations consider all system components when developing a DR plan. First, it recommends assessing the computer room environment by securing it with climate control and and backup power supply. Then it recommends a company review

its hardware solutions—including networks, servers, desktop and laptop computers, wireless devices and peripherals. Next, ensuring connectivity to a service provider is key, making sure there is redundancy.

Developing a reliable data backup system has become a necessity and, while on-site redundancies have their place, according to DHS, there is no excuse for not having an off-site backup solution in the cloud as well. These solutions address security concerns and make data recovery easier in case of emergency or disaster.



2

Keep it Current

Research has shown that only three percent of companies that suffer disasters without BC and DR plans in place survive beyond five years. If the plan isn't current and accurate, it may not be worth the paper it's printed on. Making sure your plan is reviewed on a continual basis is an important step in the process.

3

Building the Plan Foundation

To get BC and DR to work together, it's a best practice for the policies and procedures to be developed at the corporate level. Then at the departmental level BC plans can be written and individual roles and responsibilities developed and defined. Departments should have BC plans accounting for all outages—more specifically people (pandemic), places (building/work places) and processes (systems and operations).

This approach requires flexibility, and exercising that flexibility makes BC and DR that much more effective. Not every department will have the same BC and DR requirements, so a one-size-fits-all approach is not going to work.

Finding a departmental plan writer is a task that deserves significant thought. One approach is to have the corporate continuity and recovery teams recruit senior individuals at the departmental level to take charge of the project.

Putting together a cross-departmental BC and DR team—to include both IT and operations-focused employees—is an important part of executing the plan. The team should be briefed and ready to act when called upon. Emergency contact information of team members should be included within the plan itself.

Other key elements to BC and DR plans include: incidents that would launch the plans; steps to be taken if an event occurs; processes and technologies to be protected; recovery time objectives; lists of key vendors, stakeholders and regulators; and step-by-step procedures for various BC and DR activities.

4

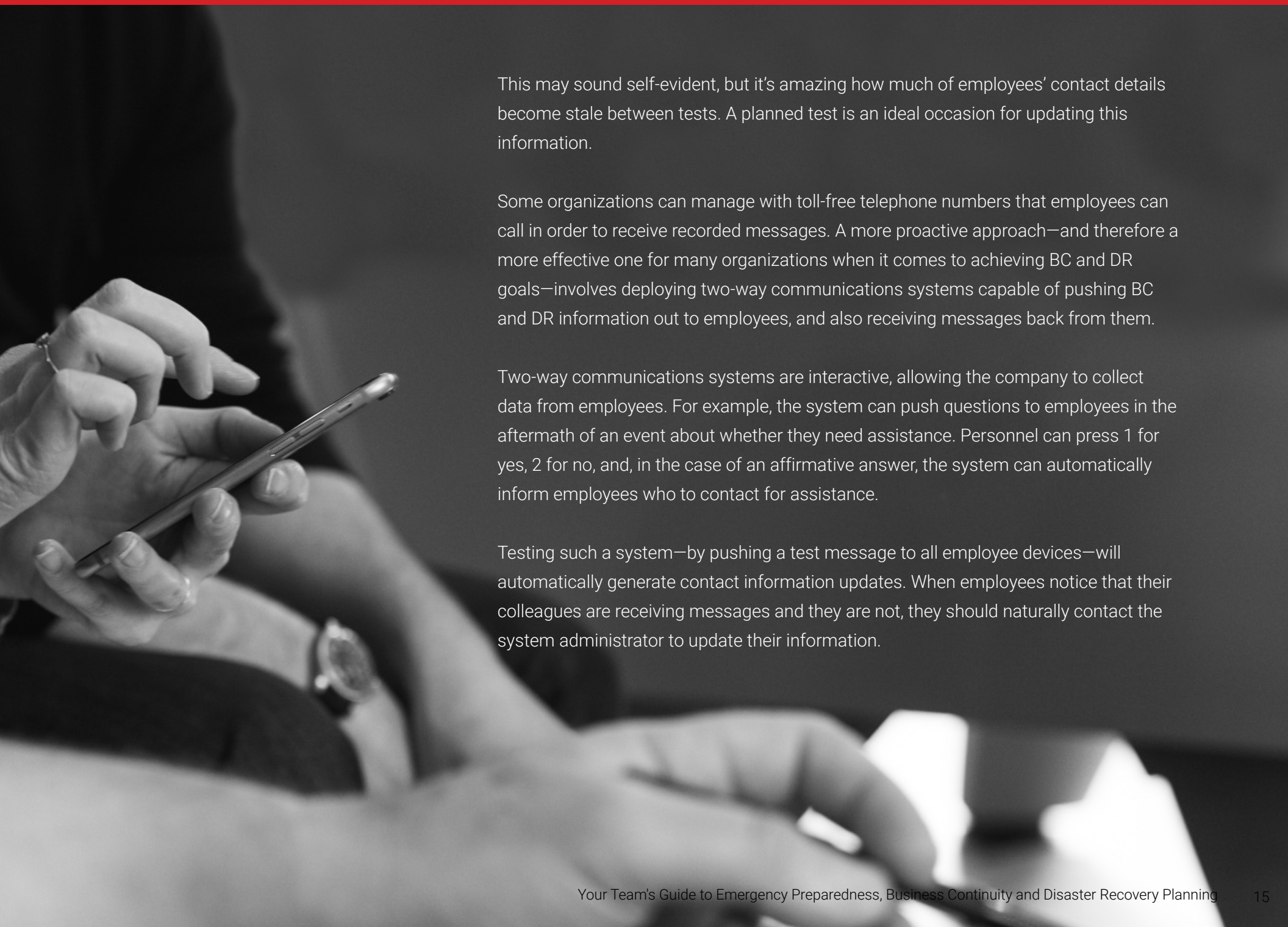
Testing and Training

Having plans in place and being able to execute on them are two different things. Successful execution will depend on testing the plan and training employees.

Successfully executing a plan increases exponentially with testing. It is considered a best practice to test BC and DR plans at least annually so employees and other stakeholders are primed to act in case of an emergency. Some companies will decide that testing should be held more than a once-a-year.

Testing helps keep plans up to date and enables a process of continuous improvement. It allows leaders to evaluate the state of company BC and DR processes to determine whether new strategies, technologies or capabilities should be implemented and whether the existing plans cover the company's current needs. New strategies and technologies may have emerged since the last test and the testing process may reveal the need to amend or even to overhaul the business continuity and disaster recovery plans.

The first step will often involve testing the effectiveness of how the company communicates with employees in an emergency event (internal communications are key to keeping workers safe, minimizing business downtime and expediting the process of getting operations back up and running). This requires having up-to-date contact information—to include home, office and cell phone numbers and personal and business email addresses—for all employees.



This may sound self-evident, but it's amazing how much of employees' contact details become stale between tests. A planned test is an ideal occasion for updating this information.

Some organizations can manage with toll-free telephone numbers that employees can call in order to receive recorded messages. A more proactive approach—and therefore a more effective one for many organizations when it comes to achieving BC and DR goals—involves deploying two-way communications systems capable of pushing BC and DR information out to employees, and also receiving messages back from them.

Two-way communications systems are interactive, allowing the company to collect data from employees. For example, the system can push questions to employees in the aftermath of an event about whether they need assistance. Personnel can press 1 for yes, 2 for no, and, in the case of an affirmative answer, the system can automatically inform employees who to contact for assistance.

Testing such a system—by pushing a test message to all employee devices—will automatically generate contact information updates. When employees notice that their colleagues are receiving messages and they are not, they should naturally contact the system administrator to update their information.

5

Testing Refined: Tabletop Exercises and Active Drills

BC and DR testing can take a number of forms, and should be flexible based on individual departmental needs. In some cases, tabletop exercises—where employees gather to review who does what in case of an event—may be sufficient. In other cases, run-throughs of procedures are recommended or necessary, especially when it comes to testing the resiliency of information systems.

Run-throughs of BC plans are live activities, like fire drills. Studies have shown that active practice allows employees to better internalize procedures, train them to care more about the BC and DR processes and helps them remember procedures longer.

Testing information systems represents perhaps the most critical aspect of the disaster recovery planning process. This typically involves a complete shutdown of systems and applications, executing a failover procedure to a dedicated disaster recovery environment and then bringing the systems back up. DR testing during regular business hours is not for the faint of heart, but doing so will help validate that a company can recover its systems under actual business conditions. Company departments should test plans at least annually and test them again when changes are made to plans or systems.

6

Involving Employees

Employees play a vital role in an organization's crisis plan. Strong, tested business continuity and disaster recovery plans are designed to cover all potential major and minor disasters and set clear roles for leadership and employees alike.

It's also good to keep in mind that there is an element of employee satisfaction and security in the care that an organization takes with BC and DR. Workers who know their organization is taking care of business on the BC and DR fronts will be happier and more satisfied because they know that the company—and their jobs—will be better protected were an event to occur.

There are several ways to involve employees in the BC and DR processes. When employees own the plan, test it, leverage their useful skills and spot hazards before they become disasters, they help reduce risk and increase overall preparedness.

The most important role that employees can play during a crisis is to own the plan before an event occurs. BC and DR plans help employees understand what they need to do to get facilities, processes and team members operational and productive after a crisis. That's why employees should review the entire plan and gain familiarity with it and their respective roles.

Depending on their role or background, certain employees may be asked to take on exceptional roles in the emergency plan. Those with emergency preparation, medical or maintenance backgrounds may be asked to take specific actions during an emergency to keep facilities running or provide safety and medical services. Many people know CPR and can play a first-aid role during a crisis.

Employee awareness is a key training activity laid out in the international standard ISO/IEC 27031 Section 7.5, which states that training should have two goals: (1) "to regularly promote DR awareness in general," and (2) to "assess and enhance competency of all relevant personnel…" All employees should be involved in active and ongoing BC and DR awareness programs.

7

Supplying and Servicing Customers

Any emergency or incident that requires BC and DR planning may also put supplies and inventory in jeopardy. That's why a growing number of companies ask their suppliers about their BC and DR plans, seeking assurance that those suppliers will be there for them in case of a catastrophic event.

There are a number of strategies that companies can employ to guard against inventory shortages. These require not only planning but, in a sense, execution before the fact, because they prepare a company in the event of a disaster.

Most companies seek to keep their inventory levels as lean as possible to save money and to minimize required storage space. But the BC and DR perspective is somewhat different: suppliers need to consider what levels of inventory they need to keep on hand—and for which specific products—to help customers avoid short-term supply disruption in the event of a worst-case scenario.

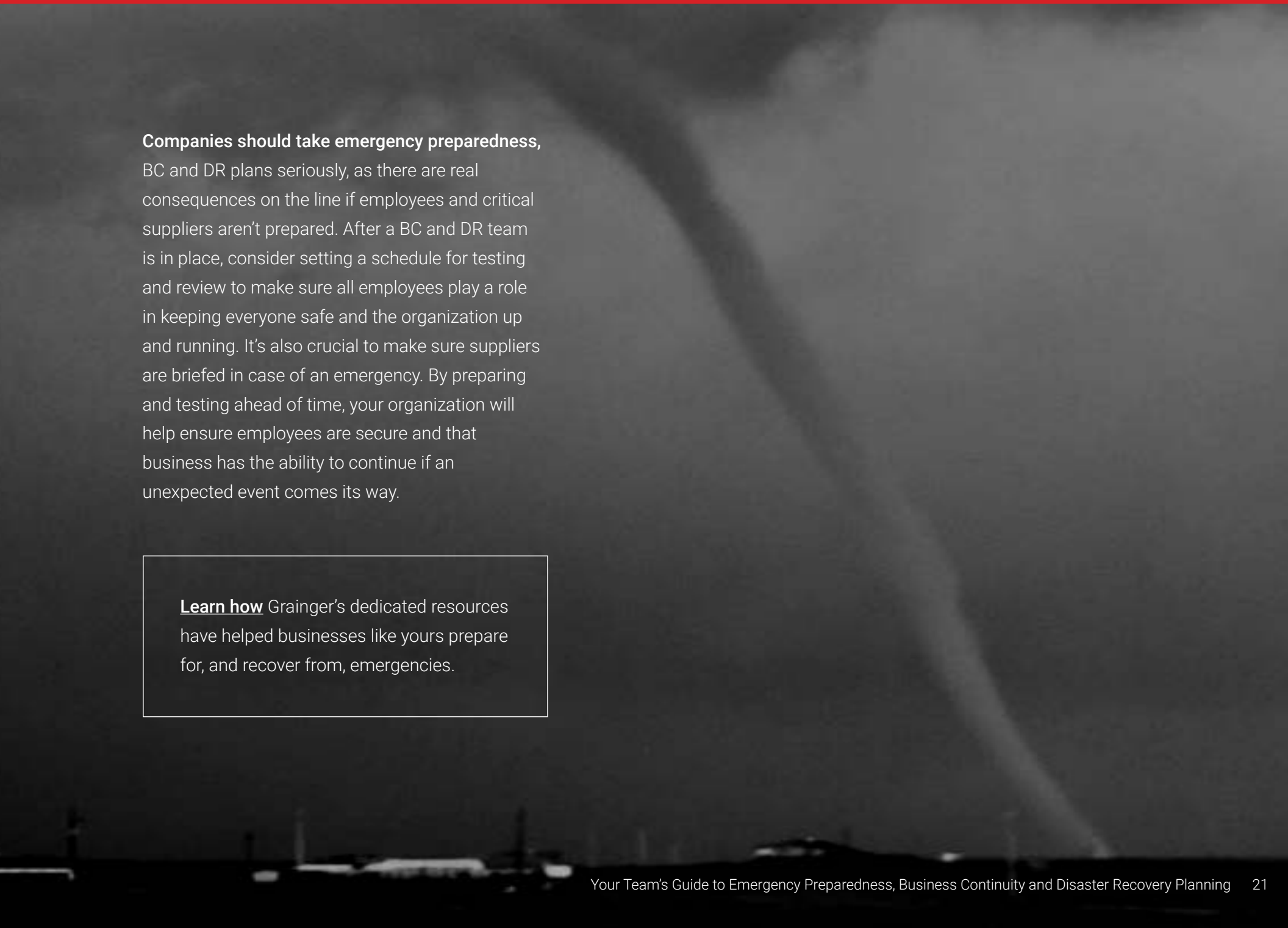
One way to handle this is by maintaining an adequate stockpile of critical products. Corporate and supply-chain management teams should keep an eye on inventory and if those supplies begin to reach critically low levels, they should reach out to suppliers to ascertain their inventory and to secure additional supplies as needed.

Diversifying the location of inventory is another best practice. Centralizing inventory of critical goods will do a company no good if, for example, an earthquake hits its warehouse location and swallows up all of its inventory.

Second sourcing is another inventory strategy that's relevant to business continuity and disaster scenarios. Identifying an alternative source for critical products and components (even if it's more expensive) will help reduce the risk of stock-outs. That way, the product would only be unavailable if a disaster were to strike both suppliers at the same time.

If a supplier is critical to a company's business operations, especially if it can't be second-sourced, it's important to know that the company has business continuity and disaster recovery plans in place. These should be available for your company to review in order to ensure that they are practical and that they will help minimize disruption to customers.

Leaders should also remember that they may be able to lean on their own suppliers in the case of an emergency, both for critical inventory and to recover information systems. Data streams, data security services and applications can be hosted and managed by vendors and accessed at primary business sites or at alternate sites using a web browser. "If an outage is detected at the client site by the vendor," a DHS document notes, "the vendor automatically holds data until the client's system is restored."



Companies should take emergency preparedness, BC and DR plans seriously, as there are real consequences on the line if employees and critical suppliers aren't prepared. After a BC and DR team is in place, consider setting a schedule for testing and review to make sure all employees play a role in keeping everyone safe and the organization up and running. It's also crucial to make sure suppliers are briefed in case of an emergency. By preparing and testing ahead of time, your organization will help ensure employees are secure and that business has the ability to continue if an unexpected event comes its way.

Learn how Grainger's dedicated resources have helped businesses like yours prepare for, and recover from, emergencies.

There are a number of strategies that companies can employ to guard against inventory shortages. These require not only planning, but, in a sense, execution before the fact, because they prepare a company in the event of a disaster.

Most companies, for good reason, seek to keep their inventory levels as lean as possible to save money and to minimize required storage space. But the BC/DR perspective is somewhat different: suppliers need to consider what levels of inventory they need to keep on hand—and for which specific products—to help customers avoid short-term supply disruption in the event of a worst-case scenario.

Grainger makes sure it has an adequate stockpile of critical products to enable the company to respond to large events. Corporate and supply-chain management teams keep an eye on that inventory and if those supplies begin to reach

critically low levels, they reach out to suppliers to ascertain their inventory and to make arrangements to secure additional supply as needed.

Diversifying the location of inventory is another best practice. Centralizing inventory of critical goods will do a company no

good if, for example, an earthquake hits its warehouse l ocation and swallows up all its inventory. Grainger helps its customers mitigate the risk of inventory loss with a menu of supply-chain services.

Second sourcing is another inventory strategy that's relevant to business continuity and disaster scenarios. Identifying an alternative source for critical products and components (even if it's more expensive) will reduce the risk of stock-outs. That way, the product will be unavailable only if a disaster were to strike both suppliers at the same time.

If a supplier is critical to a company's business operations, especially if it can't be second-sourced, it's important to know that it has business continuity and disaster recovery plans in place. These should be reviewable, to ensure that they are practical and that they will help minimize disruption to customers. Grainger puts together action planning teams that contact suppliers to understand their stocking levels and to communicate with internal procurement teams to make sure that inventories are up to required levels.

Learn more about Grainger KeepStock Inventory Management Solutions.

W.W. Grainger, Inc., a Fortune 500 industrial supply company headquartered in Lake Forest, Illinois, is a broad line, business-to-business distributor of maintenance, repair and operating (MRO) supplies, serving over three-million businesses and institutions worldwide with offerings such as motors, lighting, material handling, fasteners, plumbing, tools, and safety supplies, along with inventory management services and technical support. The company operates a network of more than 250 branches and 13 distribution centers, as well as online channels like Grainger.com, KeepStock and eProcurement.