BusinessManagement DAILY

AUGUST 19, 2020

Essential steps to creating an emergency plan for your business

As the COVID-19 pandemic has shown, employers must have an emergency plan to quickly adapt to changes. Without proper risk management, employers can be caught off-guard – with catastrophic consequences. Even after the COVID-19 national emergency is over, risks remain. COVID-19 hot spots may reemerge. Some schools may suddenly switch to remote learning when a teacher tests positive. Everything from natural disasters (fires, hurricanes, tornadoes) to illness (Bad flu year, another surprise pandemic), and civil unrest may threaten employee safety or cause physical damage to the workplace. The key to risk management is to have a solid contingency plan in place that can be scaled up or down depending on the disaster.

Risk assessment

A key resource for employers is Ready.gov, a government website focused on emergency preparedness and planning. Ready.gov suggests employers conduct risk assessment to determine the most likely hazards facing your business. Then perform a Business Impact Assessment that addresses issues like:

- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans

The website contains sample business impact assessment surveys that should be circulated to managers when developing the emergency plan. The goal is to develop a business continuity plan. Ready.gov suggests four steps to develop the business continuity plan:

- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement plans to recover critical business functions and processes.
- Organize a business continuity team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Think Big

Our thoughts are currently focused on COVID-19 and the pandemic. But we shouldn't forget the numerous hazards that can affect a business. As recent hurricane Isaias showed, it's quite possible to have a disaster interrupt another disaster with deadly consequences. Other recent reminders that contingency planning is essential are the sudden occurrence of massive protests and even civil unrest. Ready.gov lists the following potential threats.

Natural hazards

Geological hazards

- Earthquake
- Tsunami
- Volcano
- Landslide, mudslide, subsidence

Meteorological hazards

- Flood, flash flood, tidal surge
- Water control structure/dam/levee failure
- Drought
- Snow, ice, hail, sleet, arctic freeze
- Windstorm, tropical cyclone, hurricane, tornado, dust storm
- Extreme temperatures (heat, cold)
- Lightning strikes (wildland fire following)

Biological hazards

- Foodborne illnesses
- Pandemic/Infectious/communicable disease (Avian flu, COVID-19, H1N1, etc.)

Human-caused events

Accidental

- Hazardous material spill or release
- Nuclear power plant incident (if located in proximity to a nuclear power plant)
- Explosion/Fire
- Transportation accident
- Building/structure collapse

- Entrapment and or rescue (machinery, confined space, high angle, water)
- Transportation Incidents (motor vehicle, railroad, watercraft, aircraft, pipeline)

Intentional

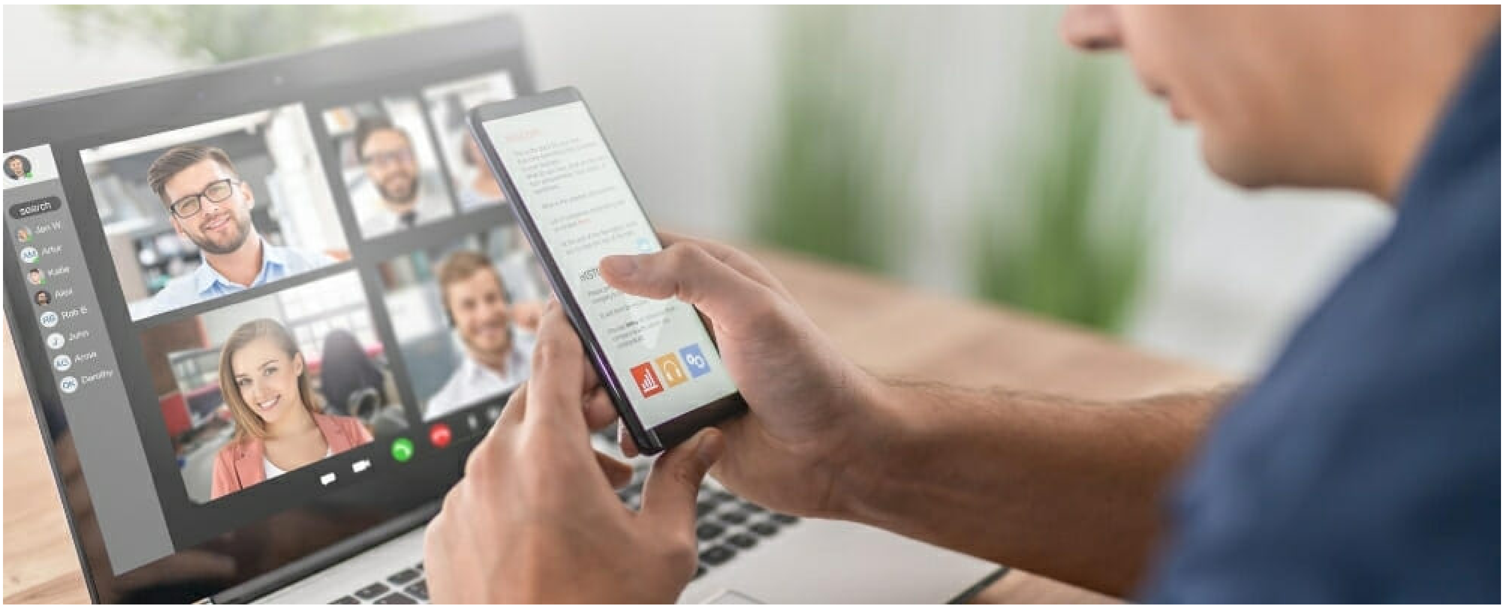
- Robbery
- Lost person, child abduction, kidnap, extortion, hostage incident, workplace violence
- Demonstrations, civil disturbance
- Bomb threat, suspicious package
- Terrorism

Technology-caused events

- Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewerage system, other critical infrastructure)
- Cybersecurity (data corruption/theft, loss of electronic data interchange or e-commerce, loss of domain name server, spyware/malware, vulnerability exploitation/botnets/hacking, denial of service).

Build an Emergency Response Team

A part of any emergency plan includes delegating specific responsibilities to key personnel. Because responding to an emergency could potentially place an employee at risk, the Occupational Safety and Health Administration has standards employees must meet depending on their duties and the specific industry involved. Employers should go to www.osha.gov to find all relevant training and steps they should take before exposing employees to any possible hazards.



Telecommuting during an emergency

As the pandemic showed, employees may have to telecommute during an emergency. This may be for brief periods (snowstorm, major protest) or longer periods (pandemic, government-ordered closures). Fortunately, organizations with a good contingency plan including telecommuting effectively manage most risks because the solution is likely telework. That's true for pandemics as well as riots, hurricanes, terror attacks, and other emergencies that shut down physical workplaces.

Managing remote employees creates many unique challenges and opportunities. Employers may see increased productivity and reduced costs when they allow a remote work option. But they need to set telecommuting rules to clarify management and employee expectations. These rules should be included in a telework agreement, spelling out exactly how working from home should be done. Without clear rules, working from home may reduce rather than enhance productivity.

Warning: creating a telecommute option opens the door to Americans with Disability Act (ADA) accommodation requests to work at home. Disabled workers may request continued telework after the emergency and employers will be hard-pressed to argue it won't work.

Then there's the Family and Medical Leave Act. Allowing remote work during FMLA leave requires careful management. That's especially true after the passage of the Families First Coronavirus Response Act (FFCRA). It allows modified, partly paid FMLA leave for those whose children are sidelined by COVID-19 school and care closures. Ordinarily, when an employee is on FMLA leave, his employer *cannot* demand that the employee perform work. But under the FFCRA, that's not the case in all circumstances. Under the FFCRA, employers can offer telework as a way to curtail paid leave. However, the FFCRA also allows employers to offer intermittent leave and has to pay for the time the employee cannot telework.

Remote employees also need training in time-keeping. The Fair Labor Standards Act (FLSA) requires that employers pay for all time worked when the employee is hourly. The location of work is irrelevant. Tracking time spent answering the front door or putting in a load of laundry can mean overcounting. Conversely failing to track time spent finishing a project after kids are in bed can mean undercounting.

It's also crucial to consider safety and accident prevention. When formulating your emergency plan, include your workers' comp insurer in the discussions. They may have input into specific safety requirements.

Setting emergency remote work rules

Many businesses now have a history of working remotely. If you had a teleworking plan before the pandemic, it's time to reevaluate. What worked? What didn't? How can it be improved moving forward?

Most likely, you now know which employees performed better while telecommuting. Some employees require little supervision, others may need a more hands-on approach.

You probably have a better idea of the infrastructure and physical requirements your employees need while working remotely. Most will need a quiet space in the home, either a separate office or multi-use space.

Where social distancing requirements permit, employees may work in a co-working space. National chains providing co-work space include Regus and WeWork but there are also numerous independent locations. Again, this is only an option under certain circumstances. Include these in your contingency planning:

- **Remote Working Rules.** Will there be set office hours? When does work start and end? Can remote employees split their day? Some situations such as where the emergency also closes schools or there are widespread power and Internet outages may affect the employer's ability to set hours.
- **Technological Needs.** Will you set technology needs and standards? What type of Internet connection and speed will the remote employee need? Will secure connections such as Virtual Private Networks (VPN) be required? Who provides tech support and manages repairs and troubleshooting?
- What technology will managers and supervisors need to track time, projects and productivity? And how will they handle time-keeping and overtime for remote employees who are not exempt?

Take steps to protect intellectual property

Telecommuting presents challenges to protecting company intellectual property. The fact is, having employees suddenly work from home can mean real vulnerability for your trade secrets and other invaluable information. Here's how to address those concerns:

Contact counsel: Make sure your attorney keeps you updated on all the latest changes. Ask if your existing intellectual property and trade secret agreements are up-to-date or if there are recommended changes now that your workforce has started or is preparing to telework.

Telework agreement: Your telework agreement should include an intellectual property and trade secrets provision. Any telework agreement you have should include a set of rules specific to emergencies. The agreement should include these following basic terms:

- A statement that telework is being offered as an alternative to address the effects of a temporary emergency and that there are no promises that telework will continue.
- A reminder for hourly employees that teleworkers are expected to adhere as much as possible to core business hours. For exempt employees, you can provide more flexibility if operational needs allow.
- A robust statement on intellectual property, including a reminder of any previous trade secret or noncompete agreements the employee has signed in the past. Ideally, include a copy with the telework agreement.
- An agreement on supplies and equipment that spells out who is providing computers, printers and other equipment as well as a formula for reimbursing the employee for internet access attributed to telework. This should include designating a specific workspace for telework, if possible. (This may be difficult on an emergency basis).

IT security: Work with your Information Technology (IT) staff to assure that the teleworker's access point to company IT resources is secure. Likely they will set up a Virtual Private Network (VPN) for access or have already done so. Your VPN should protect the teleworker's equipment from access by nefarious characters (hackers and competitors, for example), your data in transit from and to the teleworker and your network from unauthorized access. If you have not used teleworkers before, get IT to secure your system ASAP.

Essential physical work

Obviously, not all work can be performed remotely. During an emergency, most organizations will still need on-site, physical work performed too. Your contingency plan must include everything from emergency physical plant shutdown to reopening. Maintenance and security are also physical jobs that need to be performed. Plus, some emergencies like violence require immediate and decisive action to prevent harm.

OSHA provides extensive help with all these. Here are some OSHA links to help with planning:

- Workplace Violence – This covers a wide range of workplace violence
- Workplace disaster planning – This covers everything from making sure exits are available to emergency workplace sheltering in place and evacuation. The page also provides information on specific threats, including COVID-19 and related illnesses.
- Workplace security guidance – This provides specific information for those security guards and other workers who must respond to emergencies.