

When You Stop Shoveling, Start Preparing: *Next Week is Severe Weather Preparedness Week*

The first week of March (3/3 to 3/9) marks the second annual national Severe Weather Preparedness Week. It's also Severe Weather Awareness Week for the states of Kansas and Missouri. In partnership with its states and others, FEMA Region VII is making plans to spread preparedness messaging to young and old throughout Iowa, Kansas, Missouri and Nebraska using traditional and social media. We ask you, our private sector partners, to help us "spread the word."

From coast to coast, all FEMA offices, with help from the states they support, as well as other organizations and partners, will deliver messaging from www.ready.gov about how to get prepared for flooding, tornadoes, wildfires, severe thunderstorms, etc. Region VII will echo daily central themes set up by FEMA headquarters in Washington D.C. around the idea that every person should "*Be A Force of Nature.*"

Daily national themes include an introduction to the week on Sunday, Mar. 3, and then on Monday, "know your risk" is discussed. On Tuesday, messaging will focus on how to "develop an emergency plan." Wednesday's theme is "build an emergency supply kit." On Thursday, NOAA weather radios will be promoted, alert notifications will be discussed and people will learn appropriate ways to respond to them. The theme for Friday is "get involved." Throughout the week, we'll remind individuals and businesses that by preparing they become an example to others and help to motivate them to prepare too. Check out daily messages all week on www.Twitter.com/FEMARegion7.

Amid the coordinated theme-based messaging, FEMA Region VII will also engage followers in discussions about creating and tailoring Twitter lists BEFORE an emergency so individuals and businesses will have their own "virtual emergency information toolkits."

Businesses are encouraged to participate in these discussions and help FEMA promote the idea of building emergency Twitter lists and to support any or all of the preparedness messaging for the week. For more information about FEMA's social media outreach and policies, visit www.fema.gov/social-media.

Information about Kansas and Missouri events and messages for the week can be found at www.Twitter.com/KansasEmergency and www.Twitter.com/mostormaware.



Shaking the tree: A Missouri man prevents tree limbs from snapping under weight of snow. FEMA photo by Barb Sturner.

Understanding the Risks of Carbon Monoxide

Can Prevent Tragedy

“Police and fire crews investigated two people who may have died from carbon monoxide poisoning in Kansas City, Kan. Emergency crews took readings inside the home where carbon monoxide levels were ‘dangerously high.’” (“Siblings dead from apparent carbon monoxide poisoning,” WDAF TV, Kansas City, MO, Feb. 26, 2013)

Recent news reports on fatalities that may be related to carbon monoxide (CO) have prompted many in the area to redouble efforts to inform the general public of the dangers of CO, particularly during times of severe winter weather and power outages.

CO is an odorless, colorless gas that can cause sudden illness and death. CO is produced any time a fossil fuel is burned in a furnace, vehicle, generator, grill, or elsewhere. CO from these sources can build up in enclosed or semi-enclosed spaces and poison the people and animals in them.

You Can Prevent Carbon Monoxide Exposure

- **Do** have your heating system, water heater and any other gas, oil, or coal burning appliances serviced by a qualified technician every year.
- **Do** install a battery-operated or battery back-up CO detector in your home and check or replace the battery when you change the time on your clocks each spring and fall. If the detector sounds leave your home immediately and call 911.
- **Do** seek prompt medical attention if you suspect CO poisoning and are feeling light-headed or nauseous.
- **Don't** use a generator, charcoal grill, camp stove, or other gasoline or charcoal-burning device inside your home, basement, or garage or near a window.
- **Don't** run a car or truck inside a garage attached to your house, even if you leave the door open.
- **Don't** burn anything in a stove or fireplace that isn't vented.
- **Don't** heat your house with a gas oven.

PORTABLE GENERATORS: Portable back-up generators produce the poison gas carbon monoxide (CO). CO is an odorless, colorless gas that kills without warning. It claims the lives of hundreds of people every year and makes thousands more ill. Follow these steps to keep your family safe.

- Never use a generator inside your home or garage, even if doors and windows are open.
- Only use generators outside, more than 20 feet away from your home, doors, and windows.

OIL & GAS FURNACES: Every winter when the temperature drops, your furnace can become a silent killer. Gas- and oil-burning furnaces produce carbon monoxide (CO). CO is an invisible, odorless, poison gas that kills hundreds every year and makes thousands more sick. Follow these steps to keep your family safe this winter.

- Have your furnace inspected every year.

CO DETECTORS:

- Install battery-operated or battery back-up CO detectors near every sleeping area in your home.
- Check CO detectors regularly to be sure they are functioning properly.

For more information on CO dangers and prevention, log on to www.cdc.gov/co/default.htm . (Source: HHS, Centers for Disease Control and Prevention.)

Employers Mull Workforce Safety Policies During Snowstorms

With two fatalities reported already from snowstorms in Region VII, the watchful media has occasioned discussion on employee safety policy. In Kansas, two drivers were killed during the commuter rush hour. Some employers seem ill-prepared for snow and resistant to grant snow days, or work-from-home days. Others announce automatic closures. As is often the case, preparation can resolve competing interests.

“When conditions scream ‘Take a snow day!’ many workers struggle with the decision,” reports the Kansas City Star. “Even when employers say they stress safety first, there can be pressure to show up if the workplace is open.”

Employers should prepare in advance of snow days to make arrangements to ensure the safety of staff. Leigh Branham, an employee engagement consultant at *Keeping The People* in Overland Park, agrees that employers need to determine ahead of time who is mission-critical and how these employees can get to work. “Area hospitals are good at that,” the Star reports. “They bring in cots or reserve hotel rooms and have transportation procedures to get and keep essential employees on site. St. Luke’s Hospital, for example, housed more than 300 employees in last week’s storm and expected to do the same if conditions warranted this week.

Balancing Business and Worker Safety

According to Jim Nimmo, general manager of El Patron Cocina & Bar, it is important to ensure that staff can get to and from work safely. “Until it actually starts snowing we have to be open if you want to continue to run a restaurant that stays open and does well,” he said. “If it starts snowing tonight we will be sending people home very quickly. I am very concerned about the safety of my staff and very concerned about them getting home safe. I’m not endangering my staff just to make sure someone gets a taco. But the other side of that is — we are a business that also needs to be alert to the needs of our guests.”

At Legends in Kansas City Kansas, all shops were automatically closed due to the snowfall. The “top priority is always the safety of the all customers and employees,” officials said in a statement this afternoon.

(Source: Kansas City Star, “Storm puts employees in tough spot about going to work, Mon. Feb. 25, 2013, by Dianne Stafford.)



Severe weather sentinels: Snowmen line boulevard in Olathe, Kansas.

Photo by Bonnie R. Weinberg

Winter Weather Safety Tips

The Midwest is no stranger to extremely cold winters. Winter storms can be accompanied by dangerously low temperatures, strong winds, icing, sleet and freezing rain. While the danger from winter weather varies across the country, nearly all Americans, regardless of where they live, are likely to face some type of severe winter weather at some point in their lives. The National Weather Service refers to winter storms as the “Deceptive Killers” because most deaths are indirectly related to the storm. Instead, people die in traffic accidents on icy roads and of hypothermia from prolonged exposure to cold. It is important to be prepared for winter weather before it strikes.

To prepare for winter storms, you should add the following items to your emergency kits:

- Rock salt to melt ice on walkways.
- Sand to improve traction.
- Snow shovels and other snow removal equipment.
- Sufficient heating fuel.
- Adequate clothing and blankets to keep you warm.
- Minimize travel.



FEMA photo by Stephenie Adams.

To learn more about winter preparedness, please visit

www.ready.gov/winter-weather .

New Kevlar-Reinforced *StormRoom* Can Withstand 250-MPH Winds

Severe weather preparedness goes beyond buying batteries and stocking up on bottled water. During a severe storm, windborne debris ranging from broken building materials to common household items can become flying missiles. Masonry, framing and sheet rock alone may not stop this kind of threat. If a tornado suddenly appears on the horizon, it is critical that families have a secure shelter.

The DuPont Corporation has created a new safe room, called the StormRoom™. The new invention makes use of Kevlar™, a high-strength fiber developed by DuPont in 1965. Kevlar uses include body armor and racing tires.



The DuPont StormRoom is the only in-home shelter reinforced with Kevlar similar to the bullet-resistant material used to protect police and military personnel. Kevlar-reinforced walls create a virtually impenetrable barrier to protect families from flying debris during a tornado or, in coastal areas, a hurricane. The StormRoom is designed to endure wind speeds of up to 250 miles per hour. Independent tests show that the StormRoom withstood repeated hits by building timbers fired at speeds equivalent to those experienced in Category 5 hurricanes and EF-5 tornados. The StormRoom is anchored to concrete foundations with chemically set anchors strong enough to help resist the wind uplift generated by the most powerful storms.

For more information about the StormRoom, log on to:

http://www2.dupont.com/Stormroom/en_US/products/Products_subpages/proven_by_science.html .

Stafford Act Amendment Elevates Tribes

Federally Recognized Tribes Can Request Aid Directly from President

On January 29, 2013, President Obama signed into law the Sandy Recovery Improvement Act of 2013 (P.L. 113-2) (SRIA) which includes an amendment to the Stafford Act authorizing a federally recognized Tribe to make a direct request to the President for a major disaster or emergency declaration.

Prior to the amendment, a state disaster declaration was needed in order for a Tribe to receive disaster assistance, and Tribes were largely considered on par with a local government in terms of the administration of federal disaster assistance.

“This amendment to the Stafford Act follows on the President’s commitments to Indian Country, strengthens the government to government relationship between FEMA and federally recognized Tribes, and will enhance the way FEMA supports Tribal communities before, during, and after disasters,” FEMA Administrator Craig Fugate said.

The amendment also provides that Tribes may elect to receive assistance under a State’s declaration, provided that the President does not make a declaration for the Tribe for the same incident.

It also authorizes the President to establish criteria to adjust the non-federal cost share for an Indian tribal government consistent to the extent allowed by current authorities.

It also requires FEMA to consider the unique circumstances of tribes when it develops regulations to implement the provision. The amendment includes federally recognized Indian tribal governments in numerous references to state and local governments within the Stafford Act.

FEMA is currently developing specific implementation procedures for this authority and will provide further guidance through a combination of rulemaking and the development of policy or other guidance documents.

Survey: Small Businesses Underestimate Cyber Threat

Small businesses, by a wide margin, underestimate the threat of crippling cyberattack, according to a study by the National Cyber Security Alliance (NCSA) and Symantec. They found that 77 percent of 1,015 small businesses (less than 250 employees) think they are safe from cyber attacks. However, of this 77 percent, 83 percent do not have a cybersecurity plan in place even though they are relying more and more on technology such as cloud services and social media to conduct business.

The survey also found many areas in which small businesses had issues, such as establishing Internet security policies and practices, handling and responding to data breaches, and providing consistent IT/security management. Nearly 60 percent of respondents admitted they have no plan outlining how to respond to and report loss of data due to a breach. Many are not even feigning concern even though their digital footprint is growing. Some 66 percent said they are not concerned about cyber threats either from external hackers or nefarious employees or contractors inside their companies. The survey showed that not many employees are subject to discipline regarding Internet security and privacy. The full survey can be found at

<http://www.staysafeonline.org/stay-safe-online/resources/> .

Cybersecurity: What to Do If Your Small Business Gets Hacked

In a report released by Symantec, the maker of the Norton Anti-Virus software, 36 percent of the global targeted attacks in the first half of 2012 were directed against small businesses with 250 or fewer employees.

FOXBusiness.com spoke to four cyber-security experts to create a 5-step plan that will get you safely up and running again in no time if and when your business is compromised by a hacker.

No. 1: Identify Whether an Attack Has Occurred

Rob Lee, the Digital Forensics and Instant Response Lead at the SANS Institute (a leading information security training institute), says that identifying whether a hacking attack has occurred is incredibly challenging for most businesses. In fact, Lee referenced findings from cybersecurity firm Mandiant that showed that it takes companies an average of 416 days from the initial attack to detect a security breach. Warning signs might include machines that are suddenly running slowly or crashing, strange network usage patterns, huge transfers of data to unknown destinations or visits from unfamiliar IP addresses (for instance, visits from Eastern European IP addresses when your business's customers are all based in Texas).

No. 2: Investigate the Scope of the Compromise

The next step is to figure out how many systems or machines have been affected by the compromise, says Roesch. Unless you have an information or cyber-security expert on staff, this would be a good time to call in a professional consultant, who will be able to identify the type of attack being utilized by the hacker, conduct a network and malware analysis, and figure out which systems and data files have been compromised. A security expert will also be able to tell you whether the attack was mass-produced –something an employee might have picked up by browsing a compromised website – or whether it was a unique, targeted attack, which might suggest that the perpetrator was a competitor of some sort, says Dr. Judge.

No. 3: Contain the Attack

Once the scope of the compromise has been determined, says Lee, “all systems should be pulled offline simultaneously.” While the kneejerk response might be to pull the plug on machines as soon as a compromise has been detected, waiting until a thorough investigation has been conducted will better serve you in figuring out how to protect your system from future attacks.

No. 4: Remediate and Repair Systems to Prevent Future Attacks

After pulling your systems offline, you can reinstall programs from master discs. Then, using the information you've learned about the breach, says Hemanshu Nigam, founder of SSP Blue, a safety, security and privacy firm, “you can close the gaps in your systems, so it doesn't happen again.” A big part of the remediation process is changing your employees' behavior; Nigam identifies employees as a small business's weakest security points. “By quickly clicking into emails from strange senders or accessing infected sites, employees can lead to a security breach,” says Nigam. Dr. Judge recommends using web app firewalls, which can shield your website from attacks, and web filtering services, which will protect your employees from compromised websites that they might visit on work devices.

No. 5: Communicate Breaches Effectively

“The reality is that many companies get hacked at some point,” says Dr. Judge, “and communication with the customer base is critical.” Nigam agrees that customers should be informed to the extent possible, which will actually help build trust between your business and clients, as long as you effectively communicate that you are making all efforts to prevent another attack. Depending on what type of data has been compromised, you may also have a legal obligation to inform your consumers. This is most likely the case if personal information or financial data has been breached in any way; individual laws differ from state to state.

(Source: <http://smallbusiness.foxbusiness.com/technology-web/2013/02/19/5-steps-to-recovery-after-your-business-has-been-hacked/> .