



# Are You Prepared?

Does your company have a plan in case some unforeseen event occurs that could alter the way your business operates? If you don't, you should and there is no time like the present to develop one.

BY FRANK GASPERINI

**Editor's Note:** Frank Gasperini is the executive vice president and CEO of the National Council of Agricultural Employers (NCAE) in Washington, D.C. He has been with the organization since 2008. The NCAE is the national trade association representing agricultural employers and agri-businesses with Congress and federal agencies.

He will be retiring at the end of 2017, but before he does, he will be one of the featured speakers at the 2017 Big Grower Executive Summit, Oct. 1-3, in Wakefield, Massachusetts (near Boston).

Gasperini will discuss "What's Next on the Labor Front?" where he will address many of the employment issues facing our industry.

To learn more about the Big Grower Executive Summit, please visit [www.biggrower.com/executivesummit](http://www.biggrower.com/executivesummit).

**W**hat do a fire at a small business, global computer ransomware attacks and NCAE's planning for my retirement at the end of this year all have in common?

How is this important to your concerns as employers?

Let's discuss these three scenarios first, then tie the three together with some common steps

to mitigate, if not totally eliminate the risks so your business could move on to survive and prosper. Remember business always involves risk. We can never eliminate risk, but we certainly can manage, minimize and mitigate it.

### First Scenario

A small business in Virginia experienced a massive fire. The fire started at a neighboring business and spread quickly. Among the losses were the business's computer systems, including onsite backup, I-9 files, personnel files and current year payroll, so there is no backup from a payroll company. They have 15 employees.

The week after the fire, one employee was detained in a traffic stop and it was determined that his driver's license was not authentic. ICE has contacted the business with I-9 questions, and the owner is concerned about an open discussion with the U.S. Department of Labor Wage and Hour division pending from last year.

### Second Scenario

Over the weekend of May 13, 2017, the world learned of a major cyber-crime involving

ransomware that disrupted computers in many different industries around the world. Unlike traditional ransomware attacks, even those who paid, found that their data was lost forever.

Those who regularly maintained their computer programs, updating regularly as recommended by the software manufacturer, may have been protected. Those still using outdated operating platforms, old computers and particularly those using improperly registered software are most likely out of luck.

### Third Scenario

I will be retiring from the National Council of Agricultural Employers at the end of this year. I plan to remain engaged in the industry through my part-time management of the Agricultural Safety and Health Council of America (ASHCA). In preparing for my retirement, NCAE has organized a succession planning committee.

Key issues in succession planning differ only in the level of urgency from what we should all be considering every day to prepare for a disaster. What will happen if/when the owner — that one person who holds most of the critical day-to-day operating information, including where to find everything — is not available?

### Hope for the Best, But Plan for ...

Now, let's tie these three scenarios together. First, you have to have a plan. Second, you must work to implement the plan. Third, keep on implementing and improving the plan and its execution.

All three scenarios point to the importance of written procedure and roadmaps, including at least a one- or two-page document, like NCAE's "Frank was run over by a bus" emergency operations plan. Yes, we really have a summary of what must happen each week or month, who needs to be notified, paid, collected from, important contact, where things are located, etc.

Does your business have a document like this? If you don't, you should. Every business should have one. Even just a few pages written out can mean the difference between survival or failure of your business. Several people should know about that document and where to locate it. At least one copy of that document should be stored off-site in a place that is accessible in the event your office is destroyed.

Next, keep all of the paper you want, but in this age of computers even aging baby boomers like me can make the change to digital office keeping.

At NCAE, we learned some hard but valuable lessons when my relatively new laptop was stolen from the presenter's podium at a meeting. The lesson was not to mistrust computer records,

but that you must take security seriously and plan for backup.

For growers who rely more and more on automated programs and systems to run their greenhouses, running a true virtual office with complete 24/7 access and reliable backup systems should be second nature. You must back up everything.

We use Google Drive and Dropbox. Other options are available for around \$100 a year to back up everything in your computer automatically and allow you to recover everything if the computer is lost.

### Pay Now, or Really Pay Later

Another lesson is not to skimp on your office systems; buy quality software and spend appropriately for updated, properly licensed and registered software. How foolish the hacked business owner must feel for not having spent as little as \$150 per year for updated and authorized operating systems.

Think of how much better off the first two businesses would be if they had been keeping their records, including I-9s and payroll records, in a digital format with proper backup? Since they relied on paper records only in the first scenario, they will have to follow vague replacement procedure to re-do their I-9s, and have little to defend or justify their compliance

with the Wage and Hour division. In the second scenario, to save less than \$200 per year, some of the ransomware victims will go out of business while others will struggle to survive.

In the third scenario, if you hold all of the critical details in your head, known only to you, without which your business could not survive, or come to an orderly closure, then you have some work to do.

This is what we have been pursuing at NCAE, in addition to serving our agricultural employer constituents every day here in Washington, D.C., I am confident that NCAE is prepared for a smooth, positive, successful transition that will lead to continued, and improved, representation of grower and agricultural employer issues in 2018.

I urge you to work on your own "got hit by a bus" plan, computerizing your office and records, assuring modern and fully licensed software and operating systems, and offsite backup and storage.

Don't delay, start today. Even five minutes a day will get you where you need to be sooner than you think.

Don't wait for a disaster to make you realize how important it could have been. ■

*Frank Gasperini can be reached at frank@ncaeonline.com*

# HURST

## GREENHOUSE HEATING



Hurst boiler has been a leading choice in the Greenhouse and Nursery industries for over fifty years. Manufacturing reliable and affordable steam and hot water boilers with decades of service. Whether its conventional fuels like natural gas, oil or alternative "solid" biomass fuels Hurst offers more choices with more models to meet your heating needs with a fuel flexible solution.



[hurstboiler.com](http://hurstboiler.com)

*The Consulting Engineers First Choice*

- PELLET FUEL
- CHIP
- BARK
- SAW DUST
- MILL WASTE



The Leading Manufacturer of **GREEN Project** Wood-Fired and Biomass Boiler Systems.

**CALL** toll free **1.877.774.8778**



**HURSTBOILER** | **50 YEARS**  
 100 Boilermaker Lane • Coolidge, GA 31738-0530  
 Tel: (229) 346-3545 • Fax: (229) 346-3874  
 email: info@hurstboiler.com