



BUSINESS NEWSLETTER

PUTTING IT TOGETHER

Inside

Disaster Planning
Employee Theft
Computer Fraud
The Workers Compensation Crackdown
Cyber Liability
Employment Practices Liability
Experience Mod Changes
Terrorism & Insurance

Written and Published in House by
Durfey-Hoover-Bowden Insurance Agency

Disaster Planning



You receive a call at 4am that your building has burned down to the ground. Now what? Without a plan, you may find that your customers have moved on to greener pastures while you stumbled your way back into business.

You need to have a disaster plan. Many insurance companies provide access to guides free of charge. disastersafety.org offers a free planning tool for small to medium size businesses. As an example, we will look at a common risk in NC: Hurricanes.

It is just a matter of time before another hurricane plows through the Piedmont. A probable outcome could be days or weeks without power, internet or phone. Some advance planning can make a world of difference.

Power

Generators can mean the difference between business as usual and sitting in the dark.

What size generator?

What do you need to keep running to stay in business? Figure out the essentials and add up the wattage. There are a number of online calculators that can help with this.

Clean Power

A standard generator can fry a computer. A unit with Automatic Voltage Regulation can help minimize the chance of damage.

Gas

Gas can be hard to come by. You need to have plenty on hand. If you do not have power, chances are the gas station down the street doesn't either.

Internet

Many businesses store their information in "the cloud". This is a good solution if your building burns down, but it can be a real issue if your area loses internet for 2 weeks. If your company is very dependent on the internet, you should consider a back up plan.

- Many cell phone providers offer pay as you go mobile hotspots. Keep one around the office for emergencies. You can connect 5 to 10 computers with one device. Even desktops can connect if you purchase a USB wifi adapter.
- If you use different phone and internet providers, you may be able to have the phone system provide a backup for a low price as part of a "bundle". DHB "bundled" phone/internet and has an additional backup for close to the same price as phone alone.

Phone System/Website

- Ask your phone company about off-site voicemail. This allows for customers to continue to leave you messages during an outage.
- When the phone system goes down, most people plan to have the calls forwarded to their cell phones. You should know how to do this from the office and offsite.
- Make sure you have the ability to update your website and social media off site. This may be the best way to keep your customers up to date with your situation.

Offsite Workplace

- Do the offsite computers have the necessary software, updates and security? If employees are working from home on their own computers, you could be exposing company data to whatever virus/malware they have.
- If using a work computer, be sure it is kept up to date. You do not want to choose between spending 3 hours doing all of the necessary security updates or connecting immediately with an unsecure computer.

These are just a small sample of the things you will need to think through. Completing a plan can give you a better idea of the risks you face, and you will be better able to work with us to ensure you have the coverage that fits your needs.



Employee Theft

The opportunity to steal often comes from trust.

“I trust my employees. No one here would do that.” This response is one of the most common given when we discuss Employee Dishonesty Coverage. This came to mind when reading about a loss by a Raleigh law firm. An employee of 25 years has been accused of stealing hundreds of thousands from the company over the last 10 years. This employee had been so active in the community that a non-profit named a part of their building in her honor. Who could be more trustworthy?

Everyone trusts their employees. Why would you hire someone you didn't trust? The fact is that nearly every business experiences some degree of employee theft and the US Chamber of Commerce

reports that nearly 1/3 of all business failures result from employee crimes.

Employee theft can be much more complicated than an employee taking cash or property from the office. Just a few examples are listed below:

- Double Submission/Inflation of Expenses
- Skimming –Unrecorded Sales
- Check Tampering
- Paying Non-Existent Employees/Contractors
- Purchasing goods that do not exist.

The average case is not detected for 18 months, and the median loss was \$140,000. Research shows that the crimes

are more frequently caused by opportunity than need. Employee Dishonesty coverage can provide you with protection from this type of loss, but the most important step is prevention.

Run background checks on new employees, supervise your employees, conduct audits and look out for the warning signs of fraud. These signs can include never taking vacations (this is when the discrepancies are often found), refusing to let others touch their work, living beyond their means, missing financial records and other unexplained behavior. You should be reviewing the bank statements when they come in and questioning what you see.

The decision to press charges against an employee can be one of the hardest an employer has to make. Good financial controls can prevent it from ever happening.

Sources:

afce.com, inc.com, sba.gov

Hacking Your Bank Account is Easier Than You Think

Just a few clicks away from an empty bank account.

Small Business owners have become the low hanging fruit for cyber criminals. They have substantial assets and lack the security of large firms. Many small business owners have given little thought to protecting their computer system and often have a delay in updating the latest security software.



A good example of the risk is the Spyeye “Trojan horse” software. The software can install without you knowing just by visiting a website or viewing an email. It will monitor your activity and record your information when you log into your bank. Your login information is sent overseas and the information about your accounts is also recorded. Your money is wired overseas, but if you log back into your bank's website, it will adjust the numbers and act as if the money is still

there.

If it takes you too long to notice, the bank will not refund your money.

There is no substitute for solid security practices, but even the Pentagon has been hacked. Computer Fraud coverage can help protect against this type of risk.

Good examples of this risk were highlighted by the NY Times in the article linked below:

<http://goo.gl/toZQs>

North Carolina's Workers Compensation Crackdown



You may have seen the series of Articles the N&O ran on the problems with North Carolina's Workers Compensation coverage in 2012. This brought some of the issues with workers compensation into the forefront, and changes are being proposed.

There are two main issues that they are working to resolve.

Lack of Enforcement

NC Companies with three or more employees are required to carry workers compensation coverage. The issue is that there has not been a central authority closely monitoring this. Few companies dodging the law were caught until one of their employees was seriously injured. The N&O report indicated that up to 30,000 NC employers were breaking this law.

Since the N&O stirred the government into action, penalties assessed against businesses have increased substantially. The Charlotte Observer reported that the Industrial Commission assessed \$79,025 in fees in 2011. In the twelve months following the report, the penalties assessed increased to \$6,500,000.

The Industrial Commission has reported that it is now working to use data from the State Division of Employment Security and the NC Rate Bureau to allow them to

monitor and catch employers breaking the law. Penalties for failing to carry the coverage are between \$50 and \$100 a day.

Independent Contractors

Companies that carry Workers Compensation can avoid being charged for employee payroll by calling workers "independent contractors". Business owners have the option to exclude themselves from

coverage. If a business claims that everyone who does work for them is an independent contractor, they can have a policy that essentially covers no one. This is called a "Ghost" policy.

This is usually done to meet contractual requirements that require proof of workers compensation coverage. If the owner and "independent contractors" all buy these ghost policies, you have a large collection of policies that do close to nothing.

This leaves many without coverage, and too many people being called contractors are actually employees.

Many people think that they can decide if they want someone to be an independent contractor or em-

ployee. This is not the case. Even having someone sign a contract stating that they are an independent contractor does not count.

There is a test used by the IRS to determine the actual relationship. If your "independent contractor" is

injured and goes to the industrial commission, you could find yourself in hot water. We have included a copy of this test on the next page.

There have been proposals to remove the option for business owners to remove themselves from coverage and plans to take a closer look into who really should be listed as an employee.

Companies that play by the rules and provide protection for their employees are being undercut by those that break the law. For higher risk jobs, this can be a substantial difference. A roofing company could pay up to \$35 per \$100 of payroll for their workers compensation coverage. It is easy to see why some companies have been tempted.

30,000
NC Businesses do not carry required Workers Comp coverage.

\$50-\$100
Penalty for each day a business failed to carry required coverage.



Employee or Independent Contractor?

It takes more than calling someone an independent contractor to make them one.



Many people think they get to pick if someone is an employee or independent contractor. This is not the case. This is the list of criteria used to define who is an employee vs. an independent contractor.

Behavioral Control

Types of Instructions Given

An employee is instructed about when, where and how to do work.

1. When and where
2. What tools/equipment to use
3. What workers/assistants can be hired
4. Where to purchase supplies/services
5. What work must be done by a specified individual
6. What order or sequence to follow when performing work.

Degree of Instruction

Degree of Instruction means that the more detailed the instructions, the more control the business exercises over the worker.

The key consideration is whether the business has retained the right to control the details of a worker's performance or instead has given up that right.

Evaluation System

If an evaluation system measures the details of how the work is performed, then these factors would point to an employee. If the evaluation system measures just the end result, then this can point to either an independent contractor or an employee.

Training

If the business provides the worker with training on how to do the job, this indicates that the business wants the job done in a particular way. This is strong evidence that the worker is an employee.

Financial Control

Significant Investment

An independent contractor often has a significant investment in the equipment he or she uses in working for someone else.

Unreimbursed Expenses

Independent contractors are more likely to have unreimbursed expenses than are employees. Fixed ongoing costs that are incurred regardless of whether work is currently being performed are especially important.

Opportunity for Profit or Loss

The opportunity to make a profit or loss is another important factor. Having the possibility of incurring a loss indicates that the worker is an independent contractor.

Services Available to the Market

An independent contractor is generally free to seek out business opportunities. Independent contractors often advertise, maintain a visible business location, and are available to work in the relevant market.

An employee is generally guaranteed a regular wage amount, even when the wage or salary is supplemented by a commission. An independent contractor is usually paid by a flat fee for the job.

Types of Relationship

Written Contracts

Although a contract may state that the worker is an employee or an independent contractor, this is not sufficient to determine the worker's status. How the parties work together determines whether the worker is an employee or an independent contractor.

Employee Benefits

Employee benefits include things like insurance, pension plans, paid vacation, sick days, and disability insurance. Businesses generally do not grant these benefits to independent contractors.

Permanency of the Relationship

If you hire a worker with the expectation that the relationship will continue indefinitely, this is generally considered evidence that the intent was to create an employer-employee relationship.

Services Provided as Key Activity of the Business

If a worker provides services that are a key aspect of the business, it is more likely that the business will have the right to direct and control his or her activities.

This was a shortened sample of the IRS rules. For a complete listing, visit www.irs.gov/business



One man managed to hack into NASA and the Pentagon because he wanted proof of a UFO cover-up. Do you think a group of thieves looking for money will have trouble getting into your network?

Cyber Liability

Not if. When.

Has your company experienced a cyber liability breach? At best, the answer might be “not yet,” and the exposure is excluded on a standard policy.

The reality is that security experts believe that every company has or will be hacked. Small companies often think, why would hackers bother with us? They often have low security, substantial assets, little ability to research who did it or the influence to do anything about it. A better question is why would they bother going after a big company?

This type of loss could also be as simple as a lost laptop or cell phone with personal information on it. Claims have been filed even after the lost laptop is recovered.

Many people have a third party that handles their data. Even in their hands, it is still your responsibility. Did you read your contract? Many say you have to defend them in the event of a lawsuit.

If you are hacked and personally identifiable information may have been exposed, the costs can be staggering. These may include forensic costs to figure out what was breached, notification costs, credit monitoring, lawsuits from those affected, regulatory fines and penalties. The bar for what qualifies as personal information is quite low.

The cost per customer record breached can vary. A 2012 Ponemon Institutes study put the average cost at \$194 per record.

Just completing the application for

this coverage can be a bit daunting. Insurance companies don't plan on covering a company without security practices any more than they would insure a jewelry store that keeps its diamonds in a shoe box. Even if you do not take the coverage, the application can give you a guide to some of the things you should be thinking about.

Sued by Your Employees

Justice may be blind...
but she can still leave you bankrupt.



In 2012, North Carolina was ranked #4 in the list of states with the most Equal Employment Opportunity Commission (EEOC) claims. The NC is #2 when looked at as a percentage of claims by population.

In 2012, NC had more EEOC Claims than the bottom 22 states combined.

North Carolina is an Employment-At-Will State. You can fire an employee for almost any reason, but you can't fire someone or discriminate against a job applicant based on race, color, religion, sex (incl. pregnancy), national origin, age, disability, if they filed a Workers Comp claim or because the person complained about discrimination. Allegations of violations of the laws are brought to the EEOC. The fact that NC has so many EEOC claims shows that being a "right-to-work" state doesn't take away an employee's right to sue. This risk is called Employment Practices Liability (EPLI) and is excluded on a standard liability policy.

An example we saw locally:
Two employees of different races worked together for years. They were seen as the best of friends. As workers often do, they gave each other nicknames, and everyone laughed. Years later, one of the employees quits and told the employer that it was because he was called a nickname that was racially derogatory and that management knew about it for years and did nothing. No one saw it coming.

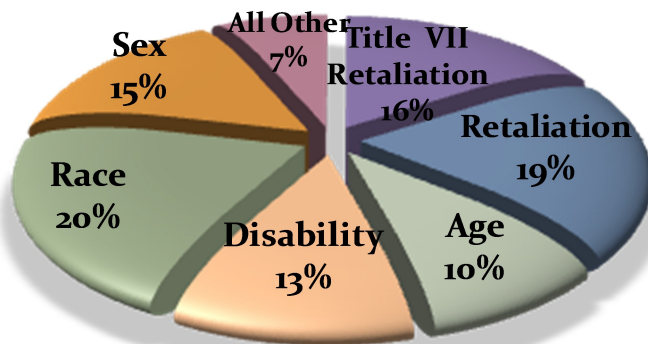
Your employee may be able to get an

attorney to sue you with no out of pocket costs. Just proving your innocence could cost hundreds of thousands. Well run businesses can be bankrupted just proving the fact that they did nothing wrong.

Accusations can range from failing to hire someone because they are pregnant to firing because they are too old.

EPLI insurance will often provide free legal advice from employment law attorneys and guide you in evaluating your current employment practices for potential law suits.

NC EEOC CLAIMS



Source: eec.gov



Terrorism & Insurance

A Complicated Relationship

As the businesses affected by the Boston bombing continue to rebuild, many have given a second thought to the need for terrorism coverage for their business. Many political figures have talked about the effect of the exclusion on Boston businesses, but few seem to understand how the coverage works.

What is an Act of Terrorism?

This seems to be a strange question, but it is at the heart of the exclusion. It depends on your policy language. The majority of policies are going to have the standard wording created by the Insurance Services Office (ISO), the organization that creates most standard policy wording.

For the ISO terrorism exclusion/coverage to apply, it needs to be a “certified act of terror”. News outlets and politicians are quick to use the word Terrorism, but even the President of the US calling something a terrorist act does not cause the exclusion to apply. The Secretary of the Treasury, Secretary of State and Attorney General all need to “certify” that the acts meet the definition. This means that there is potential for the parties involved to receive political pressure to certify/not certify the event. Many Boston businesses may be hoping that the government keeps quiet and the exclusion isn’t triggered.

What is Terrorism Coverage?

This grants coverage back for an event the three governmental agencies all call a “certified act of terror”. Insureds have the ability to reject Terrorism Insurance on some policies, but many companies do not offer that option. The coverage is available for property, liability and workers compensation.

Terrorism coverage is subsidized by the government paying 85% of covered claims, and the current plan expires in 2014. The coverage could be reworked depending on congressional action on the issue.

Experience Mod Changes

Workers compensation pricing may now be more volatile for small companies who qualify for an Experience Modifier.

What is the Experience Modifier?

Employers whose annual workers compensation premium is over \$4,000 have an “experience modifier” applied to their premium. The mod starts as a 1.0 and adjusts to be a debit to “punish” companies with worse than average losses or a credit to “reward” those with better than average losses. A company with a Mod of 1.10 would pay about 10% more than the average company. This encourages employers to emphasize workplace safety by connecting their losses directly to their premium.

How is it Calculated?

The calculation for the Experience Mod compares an individual companies payroll & losses with those that perform similar work. To limit the effect any one loss can have, the amount of the loss used in the calculation is capped. This cap had remained the same for the last 20 years and is now being adjusted up to account for the rise in medical costs. Over the next three years, the cap will be gradually increased from \$5,000 to \$15,000 and will be based on inflation after this point.

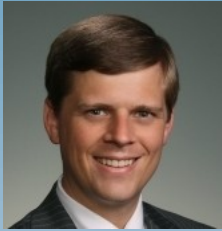
The Concern

The overall premium collected should remain the same. The change means that the “reward” or “punishment” effect can be greater. Large businesses should not see much change as the calculations average out with high payroll. The issue is that small business owners can see much larger variations in premium from year to year. Also, some companies will not hire contractors with an Experience Mod over a certain number. This can mean lost opportunities for small businesses that would have qualified under the old system.

Workplace safety efforts to prevent workplace injuries and workers compensation claims will be more influential than ever on the success of your business.



Paul Hoover IV, CPCU, CIC



Paul Hoover III, CPCU, ARM



Michael Bowden, CIC



Durfey-Hoover-Bowden

3741 Benson Dr.
Raleigh, NC 27609
Ph. 919-790-6415
Fax. 919-790-6422
www.dhbins.com