How lawyers can help businesses before — and after — disasters strike

By: Anamika Roy And Thomas A. Barstow December 13, 2018

Matthew Esworthy, partner at Bowie & Jensen, LLC

When disaster strikes businesses — be it physical damage from a storm or hackers stealing proprietary information — one of their first calls is likely to their lawyer. Whether it's preparing for a natural disaster or for a data breach, attorneys say having good policies in place and knowing what to protect is key.

Attorneys who counsel businesses on insurance matters outlined some pitfalls for companies that aren't prepared – from being underinsured to facing regulatory penalties to being ill-equipped for a rebound.

To prepare for a natural disaster, it's important to have an annual review of a company's insurance to make sure it provides adequate coverage, said Brian S. Goodman, principal at Kramon & Graham in Baltimore.

Goodman also encourages clients to have a broker review their coverage once a year.

That advice is especially true in high-flood areas as flood insurance is administered through the federal government and is separate from regular business insurance, Goodman said.

“It’s hard to get flood insurance. If you’re located on a floodplain then sometimes the government won’t underwrite it,” he said.

In the event there is any property loss after a hurricane or other natural disaster, Goodman believes it is worthwhile to hire a licensed public adjuster as the business will have to prove every element of the loss to an insurance company.

“A lot of times it’s very worthwhile,” Goodman said.

Common mistakes Goodman sees businesses make in preparing for natural disasters include: not carrying business interruption insurance and flood insurance, or not having enough coverage limits based on the value of the business, such as getting coverage for $1 million on a $3 million business.

‘Quite an undertaking’

While insurance is a big part of preparing for a natural disaster, it’s still a new frontier in cybersecurity, attorneys say.

While most carriers offer some form of cyber insurance, businesses have to take certain steps and make sure they know what they’re buying, said attorney Matthew Esworthy.

“Cyber insurance is a buzzword being thrown around, but it’s quite an undertaking,” said Esworthy, partner at Bowie & Jensen, LLC in Towson.

He encourages clients to consult with information technology experts to help them get organized and have good policies in place before seeking out cyber insurance.

“Insurance carriers are all going to want to see that anyway,” said Esworthy said.

In addition, not all cyber insurance policies are suitable for all businesses, said Nicholas J. DiCesare, an attorney who focuses on cybersecurity matters in Buffalo.

Kelly Smith Watkins

Some companies may be worried about external breaches over internal breaches by a disgruntled employee. Some coverages are only applicable if a third party sues a company for a data breach, but won't cover the investigation, said DiCesare, a partner at Barclay Damon, LLP.

It's important for businesses to take their own preventative steps before getting insurance because if a business isn't candid about their data security situation, or haven't taken the necessary steps to get the most out of cyber insurance, then the insurance company may try to get out of covering the damage if there is a breach, Esworthy said.

"All of the policies out there are going to require policy hygiene," he said.

To prepare, attorneys ask three questions about their client's data: what type of data the client is storing, what is essential to the business and what is regulated by statute or agencies that may carry additional responsibilities and what the company's obligations are if that data is compromised. The data at issue typically includes employee information, customer credit card or other personal information, schematics for designs and client lists.

"If you don't understand what you have and where it's stored, how can you possibly protect it?" Esworthy said.

After disaster hits

One common mistake companies make is failing to secure a property after a natural disaster, said Joseph S. D'Amico Jr., a senior shareholder in the litigation department

of the Lehigh Valley, Pennsylvania-based firm of Fitzpatrick Lentz & Bubba. If a fire or windstorm severely damages a building, companies should strive to ensure that no additional damage is caused by subsequent weather, vandalism or thefts, he and others said.

Further complicating matters, the stress of a situation also may cause companies to make rash decisions.

D'Amico recalled one company that didn't react quickly after a disaster and a municipality signed a demolition order, which the owner fought because he could have done the work for less. The owner would have avoided higher costs and subsequent litigation if he simply had responded immediately.

William D. Christ

Within the bounds of safety, companies should "deal with any emergency situation as quickly as possible in order to minimize the potential loss," said Kelly Smith Watkins, an attorney with Norris McLaughlin, which has offices in Allentown, Pennsylvania, New York and New Jersey.

"If a tree falls through the roof in a storm, arrange for a temporary fix as quickly as possible to avoid further damage from rain pouring in for an extended period," she said.

A lot of times, owners are reluctant to report a claim right away, out of fear they will incur higher premiums down the road. That decision can be harmful, said Dana Windisch Chilson, an attorney with the Harrisburg, Pennsylvania office of McNees Wallace & Nurick. Policies routinely include language that requires a response within a given time frame. If those deadlines are not met, coverage issues might end up in

litigation, she said. That can be avoided if a company and its attorneys understand the rules and limitations before issues arise.

“Don’t be afraid to ask,” Chilson said. “If you are covered, if you have a coverage issue, you are better to check before an event.”

And once an event occurs, documentation becomes critical. That means lining up accident reconstruction experts, consultants who understand loss issues and others who can be on call well before a storm, fire or flood, said William D. Christ, a partner with Phillips Lytle, a law firm based in Buffalo, New York.

Experienced consultants will be sure to get photos and other evidence that can help when questions arise, such as whether a roof blew off because of faulty installation, poorly constructed materials or another factor entirely.

“That is why it is important to preserve evidence,” he said. If a case goes to court, “a jury can decide who, if anyone, is at fault.”

Watkins put it this way: “Don’t go it alone.”

Tips for data protection

Technology opened digital doors into every company’s operations, making data security increasingly important in fending off ever-evolving hacking techniques.

Companies can protect themselves by taking some sensible steps, such as keeping email servers separate from other operations. For example, servers that handle sensitive customer information should be separated from computers that store credit card numbers, said Anna Mercado Clark, a partner in Buffalo, New York-based law firm Phillips Lytle.

Companies have learned the hard way that extensive steps to secure their information offer little help if a hacker gains access to their systems through third-party vendors, said Mercado Clark, who has specialized in data security issues since 2010 and is a leader in the firm’s data security and privacy and e-discovery and digital forensics practice teams.

“Think about the access you are giving to vendors,” she said, adding: “You are only as good as the weakest link in your chain.”

She recommends that companies audit their vendors’ security systems once per year.

Protecting data also means ensuring sensible backups in case of traditional disasters, such as fires and floods, Christ said. The company has specialized in data security since the 1990s.

Cloud systems that store sensitive information off-site make sense for security reasons but also as a precaution in a crisis, like when a flood hits a company's main site, Christ said.

Companies will face liability issues, too, if they haven't taken prudent steps to protect data, D'Amico said.

"Every business needs to show it has taken steps to make sure it has protected information," he said.

Questions to ask yourself

Smith Watkins suggested that companies and their attorneys ask themselves a number of detailed questions to make sure they are as protected as possible based on their unique circumstances. She offered these questions as an example:

1. Do you keep a significant amount of cash on the premises?
2. Do you have property belonging to third parties – e.g., customers, vendors or employees – on the premises?
3. What about valuable artwork or antiques?
4. What about business records and receipts?
5. How many employees do you have?
6. Do you collect and retain confidential or personal information that could fall into the wrong hands?

Once insurance is sought, different questions arise:

1. Are you required to maintain protective safeguards, such as sprinkler systems, in order for a loss to be covered?
2. How about protocols or best practices for cybersecurity?
3. Do you have an accurate inventory of everything housed on your premises?
4. Can you document/inventory items through photographs?
5. How are your business records maintained and are backup records readily available?
6. What about a copy of your insurance policies?