PROTECTING TRADE SECRETS WHEN A HURRICANE HITS DURING A PANDEMIC

July 15, 2020

By: Gavin C. Gaukroger

With more and more employees working from home or other places remotely from their normal brick and mortar office buildings, employers with protectable trade secrets have an added stress when a hurricane looms -- to safeguard their valuable confidential business and professional information from exposure or loss. The Covid-19 pandemic presents many similarities to the burdens caused by a pending hurricane. In both circumstances, employees take company resources, documents, and computing devices out of the employer's workspace. In both cases, companies that maintain their clients' private personal information, financial information, or private health information, must have a plan to effectively lock-down that data when it is otherwise accessed and used by employees remotely.

A virtual private networks (VPN) is a useful tool for managing access to e-mail services and databases, but attention should be given to employee document management practices, including whether documents can be saved locally to laptops or external storage devices. When natural disasters hit, cybercriminals, hackers, and scammers often get more active, perhaps because the ordinary course of business is disrupted, because systems may be generally compromised, or because attentions are focused elsewhere, i.e., like bringing a business back online and employees back to work. For example, when Hurricane Harvey hit a few years ago, US-CERT (now part of CISA) issued a warning that fraudulent e-mails that directed users to phishing or malware-infected websites jumped after the hurricane. Dealing with a security breach, cyberattack, or ransomware while recovering from a hurricane is likely one of the last things any business wants to face. Accordingly, companies should be prepared, during hurricane season in Florida or for new risks such as the Covid-19 crisis, with plans to maintain their businesses and protect private data before a catastrophic disaster. With human risks to key employees' health and wellness, having a backup plan to the existing backup plan would be a wise first step. In this regard, one step is to have more than one key employee informed and prepared to bring a business on-line when needed.

The words "let's call the IT guy" is not a failsafe plan. Management should have the contact information for the company's off-site data center, the Internet service provider, accounting billing processes, the credential necessary to bring an Internet-based back-office system back online as early as possible. Similarly, companies with capital investments into servers, computer systems, phone systems, and other electronics that store data should have an up-to-date inventory of their hard assets and a data map of where company data is stored and backed up. Physical records, maintained on-site at places such as at hospitals, schools, or medical service providers, should be kept safe.

If a company experiences a loss, from a natural disaster's direct effects, an interruption to their business, or a cyberattack, it should have its insurance policy at the ready so it can promptly make an insurance claim and protect its insured interests. One key element to the successful recovery of insurance proceeds is to submit comprehensive documentation of the loss to the insurance company. An insured with a claim will be much more prepared if it knows the scope of its insured interests before the loss occurs. As your grandmother told you, an ounce of prevention is worth a pound of cure – employers should take that advice to heart, especially

as we move further into this year’s hurricane season.

Related Practices

Insurance

Related Practice Teams

Dispute Resolution

Related Team Member(s)

Gavin C. Gaukroger

Topics

Trade Secrets

Hurricane Preparedness

Atlantic Hurricane Season

Hurricane Insurance Claims