CYBERSECURITY: BEFORE AND AFTER THE STORM

June 8, 2016

By: Gavin C. Gaukroger and Gina Clausen Lozier

View Full Article

Employers, healthcare providers, retailers, and virtually every other business collect data about their customers, clients, patients, and staff every day. In a data-driven economy, personally identifiable information and private health information are gathered, aggregated, stored, and protected electronically. Smart companies encrypt data and limit access to the electronic devices that store the critical financial information, trade secrets, medical information, and confidential information they collect. In many instances, State governments and Federal regulators require strict statutory compliance to ensure data security and privacy.

However, when a hurricane hits, services are disrupted and networks are destroyed, companies may find themselves scrambling to bring core business operations back on-line. Often, companies will resort to backups, work-arounds or other triage methods to limit the damage that outages can have on their business.

As part of preparations for hurricane season, companies should take stock of their computer equipment and specifically, any storage devices that may contain private, confidential data about their customers, clients, patients, and staff. Securing the physical plant and network infrastructure must be a priority. Data and security breaches can happen in a variety of ways: employee theft, computer hacking, lost or stolen equipment, or failing to wipe data from old or otherwise inactive machines. Damage, like flooding, water intrusion, or blown debris caused by a storm may physically damage devices hosting data. When a hurricane hits, the systems that your company may rely upon to protect confidential, private information may be compromised. Data security and privacy laws require that those devices be protected even in the event of a natural disaster.

Consider this circumstance: a hurricane knocks out windows and water intrusion damages your company's computers, servers and network. If the computers and servers are inoperable, is the data stored thereon destroyed and inaccessible? Probably not. Even though you may decide that the equipment is useless and appropriate for disposal, if your company stores or maintains confidential personal information, (i.e., names, addresses, driver's licenses, Social Security Numbers, e-mail addresses and passwords, private health information, insurance information, etc.,) on those devices, you need to be diligent to collect and protect the damaged equipment, and remove the confidential data from the damaged equipment before disposing or recycling it.

As an example, computers and paper documents were never recovered from a New York hospital damaged by Superstorm Sandy. Despite the belief that the saltwater intrusion would have severely damaged the computer equipment and that the paper documents were likely destroyed, the mere loss of data required the issuance of a data security breach notification to the potentially affected patients of the hospital. The New York City Health and Hospitals Corporation notified nearly 10,000 individuals, set-up a toll-free hotline and undertook an investigation into the incident.

The cost of complying with data breach notification obligations may be significant. Responsive action must be undertaken quickly. Individuals potentially affected by a data breach must be notified timely. Government regulators, including both state and Federal government agencies, must be notified. Depending on the nature of the data breach, companies often face regulatory investigations and pricey and contentious litigation from

affected individuals. Vigilance and diligence to mitigate the risk of a data breach and to manage the immediate responses are key. When a hurricane hits, protecting confidential, private data cannot be an afterthought.

The 2016 hurricane season is here and if the predications come true, it may be an active one. Take the necessary steps now to avoid getting caught in the storm. Review your physical locations to determine whether your critical computer resources are adequately protected. Contact your insurance agent to learn about ways to insure against the risks of cyberattacks, data security breaches, and storm related data loss events. Having an adequate multi-layered insurance policy can help mitigate the expenses of a data breach by providing assistance and coverage for the costs associated with the investigation and notification. There are also coverages available to rehabilitate a damaged reputation following a data breach.

If you have questions regarding data security or believe that your company has suffered a data breach, please contact attorney Gavin Gaukroger on the firm's Dispute Resolution Team. If you have questions about your insurance coverage or other policy concerns, please contact Michael J. Higer of Berger Singerman's Insurance Team.

Related Practices

Insurance

Related Practice Teams

Dispute Resolution

Related Team Member(s)

Gavin C. Gaukroger

Gina Clausen Lozier