FEB 2017

P&C PROFILE

DID YOU KNOW?

February marks the time of year when employers must post their OSHA Form 300A Injury/Illness logs in areas where employee notices are usually placed. All covered employers must post their logs for 2016 beginning on Feb. 1, and they must remain posted until April 30. The summary must list the total number of job-related injuries and illnesses that occurred during 2016 and were logged on the OSHA 300 Form.

IN THIS ISSUE

Provided by:
JRG Advisors, LLC

JRG ADVISORS

New Recommended Practices for Anti-retaliation Programs

In the wake of OSHA's new electronic injury and illness reporting and anti-retaliation rules, the Department of Labor (DOL) recently released new recommended practices for anti-retaliation programs.

OSHA currently maintains 22 whistleblower protection laws that are designed to protect employees from retaliation. According to the DOL, its recommendations should help employers to comply with these laws and create workplaces in which employees feel comfortable voicing concerns and reporting injuries and illnesses. The DOL also outlined the five most important traits of any anti-retaliation program:

1. Anti-retaliation training for employees and managers
2. Management leadership, commitment and accountability
3. A system for listening to and resolving employees' safety and compliance concerns
4. A system for receiving and responding to reports of retaliation
5. Program oversight

The DOL stated that the new recommended practices are only advisory in nature, and don't create or alter any obligations created by OSHA standards and regulations.

For more information on OSHA's new rules and anti-retaliation programs, contact us at 412-456-7000 today.

Major Climate Disasters Caused $46 Billion in Damage in 2016

Although severe weather is likely every year, there were 15 separate climate disasters in 2016 that led to at least $1 billion in damage. That's the second most severe weather events in one year since the National Centers for Environmental Information (NCEI) began tracking the costs of storms in 1980.

According to an annual report from the NCEI, various floods, droughts, wildfires, hurricanes and severe thunderstorms led to approximately $46 billion in total damage last year. Additionally, this amount doesn't account for losses due to the loss natural resources, health care costs or loss of life.

Climate-related disasters of any kind can have a large impact on businesses. Even if your business makes it through a storm relatively intact, damage to your vendors or your area's infrastructure can lead to substantial business interruption. For help preparing for a severe storm, contact your partner at JRG Advisors, LLC.

Most Cyber Attacks in 2016 Caused by Ransomware and DDoS Attacks

According to a recent report from Radware, a leading cyber security provider, nearly half of all surveyed businesses experienced a ransomware attack in 2016. Ransomware is a type of attack where an organization is "locked out" of its computer network until a financial ransom is payed, usually with the anonymous and digital bitcoin currency.

The report also showed that cyber criminals frequently used the threat of a distributed denial of service (DDoS) attack to elicit a bitcoin ransom. These attacks slow down a target server until it is rendered useless, often leading to prolonged business interruptions.

What's worse is that these types of attacks are relatively easy for criminals to perform, and are often automated by using malware or bots. Additionally, Radware found that 40 percent of respondents don't have a cyber incident response plan in place to counteract ransomware and DDoS attacks.

The report also made a number of predictions for cyber attacks in 2017, which included the creation of new types of DDoS attacks, more targeted ransomware attacks and the increased prevalence of politically-motivated cyber attacks.

Cyber Crime Evidence Connected to Russia Found in a Vermont Electric Utility System

U.S. intelligence agencies recently announced that they have discovered computer code on a laptop at a Vermont-based electric utility that can be connected to Russia. Russian sources have also been accused of influencing the most recent presidential election through cyber attacks, although it's currently unknown if the two events are connected.

Experts believe that the discovery of malicious code on a utility provider's computer network is troubling, as hackers could then gain control of and disrupt utilities on a large scale. However, there is no evidence that the code discovered on the electrical utility's laptop compromised its systems or customer information.