Cyber Risks & Liabilities

FIRST QUARTER 2020

Improve Your Cyber Incident Response Plan in 2020

In an era of constantly evolving cyber threats and advancing technology, no organization is immune to the risk of a cyber attack. According to recent survey data, 53% of percent of businesses in the United States reported being the victim of a cyber attack in 2019.

That's why having a cyber incident response plan is a vital element of any organization's approach to business continuity. At a glance, cyber incident response plans provide business leaders like you with proactive guidance to prevent cyber attacks, as well as reactive steps to follow if a breach occurs. In other words, having a cyber incident response plan can help prevent attacks from happening altogether and limit the damages in the event of a worst-case scenario.

However, simply having a cyber incident response plan in place won't guarantee cyber resilience. Rather, it's important for your organization to routinely revisit your plan to make necessary updates and improvements when new threats emerge.

Consider the following tips to adequately update and improve your cyber incident response plan in 2020:

Maintain proper documentation—Make sure your cyber risks are properly documented as a reference point for improving your incident response plan. Keep in mind that when cyber risks or threats evolve, your response plan should follow suit. Also, be sure to document any past cyber incidents that took place. By doing so, you can better analyze what went wrong and adjust your incident response plan to make sure the same concern doesn't happen again.

Prepare for different scenarios—No cyber incident is exactly the same. With this in mind, be sure your cyber incident response plan is multifaceted with tailored steps and preparations based on the type of attack. A common approach is to have varying levels of response based on the severity of the breach. For example, a phishing attack that only infected a single user and led to minimal data loss would call for a different response than a large-scale breach that resulted in significant disruption.

Test your plan—In addition to preparing for different forms of cyber attack, it's also crucial to routinely test your response plan with sample scenarios. Similar to a fire drill, try to involve every employee in the process of testing your response plan. This way, all staff members will know how they play a role, and you will be able to accurately determine the effectiveness of your plan. From there, you can make adjustments as needed and feel more confident in your plan in the event of a real cyber attack.

Wheeler & Taylor Inc.
333 Main St
www.wheelertaylor.com

Breaches of the Past Decade

Cyber attacks are an increasing threat in terms of both frequency and severity. Businesses of all sizes can be targeted by cyber attacks. Here are five of the most notable data breaches from the past decade:

Target – 2013
Home Depot – 2014
Anthem – 2015
Equifax – 2017
Marriott – 2018

Cyber Security Trends to Watch in 2020

One of the challenges of implementing reliable cyber security is that the finish line keeps being moved. As security measures continue to improve, so do the methods and tools of cyber criminals.

There is a range of possible threats to be aware of when it comes to keeping your organization cyber secure. Here are five potential risks that industry experts believe businesses should heighten their awareness of in 2020:

- **Ransomware**—Ransomware attacks can be among the most expensive for your company to have to deal with. Ransomware refers to a type of malware that can breach and encrypt the victim's files. The victim is then forced to make a ransom payment in order to regain access to their data. In addition, some attackers may also extort your company, and threaten to disclose or sell your data. Companies are advised to regularly back up all critical data and keep the backups separate from the rest of your network.

- **Phishing**—Phishing emails continue to be one of the most common causes of data breaches. This threat refers to fraudulent emails that intend to trick employees into revealing sensitive information. In 2020, phishing kit developers are expected to make it even easier for potential attackers to launch phishing campaigns. Be certain that employees are trained in anti-phishing practices and that training is regularly updated.

- **Personal device attacks**—According to a 2019 Kaspersky report, approximately half of all companies reported malware infections on employee-owned devices. With businesses continuing to increase flexibility for employees to use personal devices for work-related tasks, attackers may start targeting personal devices more heavily as a means of bypassing corporate cyber defenses. Adequate and up-to-date training is necessary for your employees. Companies should review and update their policies as they pertain to personal devices as well.

- **Third-party suppliers**—According to a survey by One Identity, 94% of organizations provide third-party suppliers with access to their network. What's more, 18% of organizations reported that a third party was to blame for a data breach. With digital connections between businesses increasing, the risk of a data breach occurring because of a mistake by someone outside of your company is also on the rise. Establish a strict security policy for all third-parties that access your network, and closely monitor that each user is only given the permissions they need.

- **DDoS attacks**—While not as notorious, DDoS attacks are about as common as ransomware incidents. Network speed increases, such as the wider release of 5G, also mean that DDoS attacks can be more difficult to stop. Have your IT department or contractor inspect devices for possible misconfigurations or vulnerabilities, and be certain that your employees are following your cyber security policies.