Arias

#AlwaysArias

FOUR RECOMMENDATIONS TO REDUCE THE CHANCES OF A CYBERATTACK

Here are some recommendations for multinational companies to follow which shall help reduce the risk of suffering cyberattacks.

MONTHLY NEWSLETTER
THE LAW FIRM OF CENTRAL AMERICA

Cyberattacks are constantly increasing in number and complexity; and this does not seem to change for 2022. This has led to many regulators to start working on introducing (or have introduced) new laws focused on both cybersecurity and data protection. However, many of these regulations (such as China's or United Arab Emirates') include data protection legislation with both, extra-territorial reach, and rigorous requirements regarding security measures to safeguard personal data.

These represents a challenge, especially for multinational companies, where trying to comply with several regulations while continuing to do business, has translated into fear of fines and reputational damage. Hence, many companies are now focusing on how to comply among different regulations while leaving room for innovation. A common approach has been to fulfill requirements for one major regulation, and then layer in the required capabilities for other regulations as needed. For example, complying with GDPR and then look to find a balance with local Latin American laws.

Due to this changing environment, many companies are both stopping the threats faced and ensuring they are up to date with the laws applicable to the data they process. To do this, here are four recommendations for multinational companies to follow which shall help reduce the risk of suffering cyberattacks:

1.Review and update policies

Companies must ensure they are up to date regarding data processing laws that apply to their course of business, while at the same time facing threats that are become more challenging and resource consuming.

Policies in place should be regularly reviewed. A new trend has shown that companies with high privacy standards are now reviewing and updating their policies every quarter. In some cases, also even third-party service providers form part of the auditing and assessment process to guarantee full compliance.

2.Training and creating awareness

It is common to hear that the user is the weakest link in the chain, and in the practice it is usually true. Therefore, the key to a good cybersecurity begins with education and awareness at all levels of the organization and with both, temporary and permanent staff, this will allow an environment with reduced risk of suffering attacks since users will be able to identify them in advance.

3.Monitor behavior and update security measures

In the same way that threats evolve and become more complex, security measures need to be updated to face them. In one hand we have physical measures, which include access to premises and hardware; and on the other hand, we have electronical measures, where companies need to have strong protocols to secure their information either directly or through third parties.

A lot can be achieved simply by monitoring the systems and detecting the threats before they happen. This vigilance may include the patching of bugs, robust filtering of internal and external communications, having a current malware defense, using codification to transfer sensitive information, among others. The specific vigilance measures will vary depending on the personal data being processed.

4.Have a data breach response plan

According to the Identity Theft Resource Center's annual report, there were 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.

Therefore, companies should consider having a data breach response plan to ensure that incidents are responded quickly and in an efficient and comprehensive way.

Many of the recent changes in regulation are now including reporting obligations and shorter report terms, which makes it harder for companies to comply. Having a data breach response plan will provide a guide on how to react once a breach has been identified.

With new privacy laws becoming effective every day, companies must be proactive and start getting a comprehensive data privacy program in place, to be able to meet the most rigorous rules. Many companies must struggle with a variety of applicable privacy laws to their business, all of which have different sets of requirements and penalties to consider, and everything indicates that these regulations will continue to grow severity and complexity in next years. Staying ahead will help mitigate cost and risk; therefore, all these actions can be the baseline for your data privacy compliance program.

Written by:

Vivian Gazel
Senior Counsel
vivian.gazel@ariaslaw.com