WE MAKE CYBER SIMPLE

DO CYBER INCIDENTS CHANGE CONSUMER BEHAVIOR?

For years the popular opinion was that people would stop doing business with companies that were breached and their information taken.

But as more and more companies were breached people didn't turn away from those companies.

That was then, this is now. Consumers in the USA report being a victim of a breach at a far higher rate than in other parts of the world, 48% versus 33%.

Adding insult to injury 5% of victims found out about the breach and the compromise of their data on the news! Companies are taking up to 6 months to notify their customers of the breach. Not only is this poor customer relations, in many cases this is a violation of notification laws.

Now 21% of people report ceasing to do business with a company that they feel isn't protecting their information and is not notifying them promptly in the event of a breach.

Customers are also notifying the company to delete all the data they have on them.

Interestingly, consumers are not in favor of big fines by regulators. They are more in favor of compensation to the victims and better cybersecurity. To confirm the better cybersecurity, consumers want mandatory monitoring of the company for 12-14 months after a breach.

This begs the question of who will do the monitoring and what will be monitored. One suggestion is to require more regulation and give people more control over how their information is gathered, stored, and used. The American Data Privacy and Protection Act (ADPPA) is our version of the General Data Protection Regulation (GDPR) from the European Union.

GDPR says that a person's data belongs to them and cannot be collected, stored, or used by a company or organization without express permission from the person. Data necessary to meet a contractual obligation or needed to deliver the service requested by the customer is an exception.

However, the request for permission must be clear, simple, and describe the specific data the company wants to collect and how it will be used. The request cannot be buried in the terms and conditions we all need to approve before using a site. The person can also specify if the data can be shared, traded, or sold. At any time, the person can request that the company delete all data about them the company has collected. The company is required to comply or state clearly why it cannot.

In short, a person's data is their property, and they have full rights to determine how it is collected, stored, traded, sold, and used.

WE MAKE CYBER SIMPLE

DO CYBER INCIDENTS CHANGE CONSUMER BEHAVIOR?

GDPR has been in operation in the EU for some time and is working well. Many people have expected similar legislation here in the USA. Of course, there will be push back by companies, especially data brokers whose existence is based upon their ability to collect and sell data about people.

But the decision will depend upon how hard people push to control their data.

If companies are held liable for the data they collect and store, then they may be more amenable to stricter rules governing it if the rules will help lower their exposure and provide an acceptable standard for protection.

Are you ready to get serious about protecting your assets and your company? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.