PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

JANUARY 28, 2020

WHAT TO DO WHEN YOUR PERSONAL DATA HAS BEEN COMPROMISED

Brandon Hemphill | Private Client Group Executive

By now, we are all intimately familiar with data breaches and cybercrime, but what can we do to prevent and recover from these incidents? Capital One, Home Depot, Marriot Hotels, and Yahoo! are all major companies that have had their data breached. The Yahoo! breach alone affected three billion people. But what do you personally do if your data was part of a breach like this? What if a cybercriminal sent that electronic invoice that you just paid? Is there anything you can do to lower the risk of your data being compromised? Could insurance help transfer these risks?

PREPARE & PROTECT

While it may seem inevitable that your personal data will be compromised, there are several things you can do to meaningfully reduce the chances and minimize disruption to your life. The most important thing you can do is practice good cyber hygiene. This includes using long and complex passwords, securing your wireless networks with WPA2 or WPA3 encryption, and installing a reputable anti-virus program on your devices.

The next level preparation is hiring a service like Rubica or K2 Intelligence to provide actively managed cyber protection for you and your family. Think of these companies and their offerings as your personal cyber secret service. They will assess your exposure and actively manage the security of your data across all of your devices.

If you are a successful individual or family and are concerned about being targeted for cybercrimes and frauds, I suggest you work with an experienced insurance broker to determine the best strategy for protecting against these kinds of losses. There are coverages available that will reimburse fraudulently disbursed funds.

continued >

These policies can provide coverage for an unauthorized transfer of funds out of your bank account. For families with children who suffer from cyber bullying, these policies can also fund the costs associated with recovery and treatment.

> The first thing you should do is find out precisely what data was stolen. When companies disclose a breach like this, they will also be responsible for communicating to their affected customers what data was compromised.

MY DATA WAS COMPROMISED, NOW WHAT?

The first thing you should do is find out precisely what data was stolen. When companies disclose a breach like this, they will also be responsible for communicating to their affected customers what data was compromised. Experts at Norton detail five types of data breaches and the appropriate responses to each, as well as seven steps you should take after a data breach. Yes, you should monitor your credit and consider taking advantage of the services and settlements offered by the offending companies and definitely change your passwords.

WHY IS THIS IMPORTANT?

When is the last time you weren't busy? Data breaches are disruptive, and being a victim of a cybercrime or extortion is scary and upsetting, especially if you just lost a meaningful amount of your hard-earned assets. The Washington State Attorney General's office has released its fourth annual Data Breach Report, and 2019 saw a 20% increase in the number of data breaches in the State of Washington. While our government at the federal, state, and municipal levels is working to hold offenders accountable and put safeguards in place, the reality is this threat is not going away.

The bottom line is, if you are informed, you may be able to prevent a major disruption to your lifestyle or reduce downtime. Talk to a trusted insurance advisor about the solutions an insurance product may be able to provide in order to make you whole after a loss and the steps you can take to prevent something like this from happening in the first place.