Hibbs ♦ Hallmark & Company

BIG "I" BEST PRACTICES AGENCY 2019

The HHC Herald

Experience you deserve from a team you can trust.

Cyber Liability Insurance

Many businesses today are increasingly exposed to a new form of liability of which they may be unaware. Cyber liability incidents are occurring in greater number and very often without the benefit of insurance to cover the loss and related defense expenses. In order to better understand "cyber liability," let's first consider the types of information at risk:

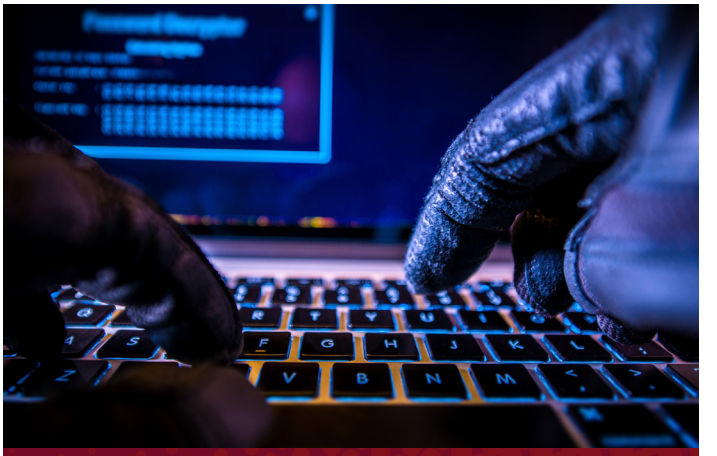
- Credit Card Information
- Personal Financial Information (Social Security Numbers, Drivers License Numbers, Bank Information, Employment and Insurance Information)
- Personal Health Information

Obviously some businesses are at greater risk than others, but hardly a week goes by that data breaches are not in the media. Common causes include: negligent release of information, stolen or misplaced laptop computers, stolen or improperly handled backup computer tapes, improperly disposed papers, malicious software, and disgruntled employees.

General Liability and Crime insurance have limited coverage because they are concerned with damage to tangible property.

Knowing that traditional insurance is not the answer, a careful review of your exposures will help to determine the type(s) and amounts of cyber liability insurance needed:

- First-Party: Direct loss due to "injury" to electronic data or systems resulting from acts of others.
  Coverage should include Crisis Management, Extortion, Restoration Costs, and Business Interruption
- Third-Party: Liability for financial losses or costs sustained by others resulting from Internet or other electronic activities.
  Coverage should include Network Liability, Electronic Media Liability, Regulatory Defense Costs, Privacy Liability
- Combination of both First-Party and Third-Party coverage.



WHO NEEDS THIS COVERAGE MOST?

This question is best answered by another question:

Who is responsible for confidential data?

Today businesses of all sorts are becoming more electronic and handling more and more confidential data. Industries such as Healthcare, Government, Financial Institutions, Schools/Universities, Online Merchants, and Church/Philanthropic Organizations are particularly exposed.

It would seem that cyber liability is no longer a matter of "if" an incident will occur but "when."

- Cyber crimes are the fastest growing crime in the United States
- More than 2 billion person records are stolen every year
- The average number of security breaches per organization was 145 in 2018
- The average number of security breaches in 2018 grew by 11% from 2017
- The average cost of cybercrime grew 12% from 2017 to 2018
- Cybercrime will cost the world over $6T annually by 2021
- Every 11 seconds, a business will become a victim of a ransomware attack by the year 2021
- 48% of malicious email attachments are office files
- Web attacks were up 56% in 2018
- Data for a single stolen credit card sells for up to $45 on underground markets

For more information:

Hibbs-Hallmark & Company
501 Shelley Drive ♦ Tyler, TX 75701
903.561.8484 ♦ 800.765.6767 ♦ www.HibbsHallmark.com