3000 INSURANCE GROUP

Cyber Liability

Ask yourself these questions and then decide if you need a Cyber Liability Insurance policy.

- If my company suffers a "Cyber Event" (breach, ransom ware, cybercrime, malware, etc.) who will I call?
- If my customer data is breached who will I contact for; Notification, Monitoring, Legal Advice for government penalties/fines, and Public Relations?
- Does my current insurance policy(s) insure against most "Cyber Events"? What are my limits/gaps?
- Does my agreement with my IT vendor include costs associated; 24 hour assistance, Cyber Event if it was human error by my employees, loss of device (laptop or smart with client data), guaranteed backup restoration within 1-2 business days?
- Is all software properly updated on a timely basis, is virus software up to date, are passwords changed on a regular basis?
- Are you responsible for your client's data if a 3rd party software you are using is breached (i.e. credit card company or a customer relations management system? If not, are you sure they have adequate insurance/financials to pay all associated damages?

What if I cannot answer the above questions?

If you can't answer one or more the above questions with confidence there is a very good chance you need a Cyber Liability Insurance policy. A Cyber Liability Insurance policy not only insures you for many different "Cyber Events", but also provides you services that help you through a crisis caused by a "Cyber Event". This is commonly referred to as a Cyber Coach (Experts provided by the insurance carrier that help guide you through the steps should a "Cyber Event" occur).

Common Cyber Events Include:

- **Data Breach –** This is the most common Cyber Event. If your data is breached it might entail; loss of income, loss of reputation, governmental fines/penalties, notification, monitoring, crisis management, data restoration, and IT forensics.
- **Extortion –** Commonly referred to as a ransom ware malware. A virus locks your system done until you pay a ransom to obtain a "password" unlocking your system. This might entail, loss of income, cost of ransom demand, and IT forensics.
- **Crime –** This is commonly referred to as phishing. An unknown hacker appears to give you/your staff instructions to transfer money for legitimate purposes by appearing to be a vendor, bank, employer, etc. This might include; loss of income, and IT forensics.
- **Media Liability –** Publishing or posting content without authorization OR slanderous content. This could result in loss of income, legal fees, and loss of reputation.

Statistics:

- **71%** of security breaches target small businesses
- **77%** of all employees leave their computers unattended
- **95%** of credit card breaches that Visa, Inc., discovers are from its smallest business customers
- **60%** among small and medium business owners that suffer a breach, a staggering 60% go out of business after 6 months.

3000iG.com | 405.521.1600 | info@3000iG.com