techrug

WHY EVERY ORGANIZATION NEEDS CYBERBREACH INSURANCE

Any company that handles, maintains or processes Personally Identifiable (**Driver's License Numbers, Social Security Numbers, Dates of Birth, Email Addresses and more**) or Protected Health (**Account Numbers, Medical Record Numbers, Insurance Beneficiary Numbers and more**) Information needs their own CyberBreach Insurance to protect their organization against claims arising out of Ransomware, a Rogue Employee, a Staff Mistake, a Phishing Attack, Theft of Hardware, Lost or Stolen Laptop or Device, and other causes of loss.

A Sample of Insuring Agreements you might want to pay attention to include:

- **Security Liability** – Covers the Unauthorized Access of a network that leads to the destruction, deletion or corruption of electronic data as well as the failure to prevent the transmission of Malicious Code from Computer Systems to third party computers and systems.

- **Privacy Liability** - Covers the theft, loss or unauthorized disclosure of Personally Identifiable Non- Public Information or Third Party Corporate Information that is in your care, custody or control.

- **Breach Response Costs** - Covers the cost of notifying parties whose data has been affected by a data breach. This coverage is important because most states have laws requiring businesses to inform individuals when their personal information has been compromised.

- **Crisis Management Expense** - If a breach does occur and your company makes the newspaper or network news, you better believe your competition will use this against you to try and take your clients. You need coverage for the costs associated to hire a public relations firm to avert or mitigate material damage against your reputation.

- **Forensic Expense** - Provides coverage for the cost of retaining an attorney to advise you of your obligations under data breach notification laws in the event of a network security breach impacting PII, as well as the cost of hiring a computer security expert to determine the existence, cause and extent of the breach.

- **Regulatory Coverage** – This coverage is for claims expenses and penalties if a governmental agency or regulatory body brings an enforcement action against you for a violation of a law protecting the confidentiality and security of Personally Identifiable Information.

- **Digital Asset Restoration Costs** - Provides coverage for the cost of restoring or replacing data, regardless of whether it is your or your client's, as a result of a security breach on your network or your cloud service provider's network

- **Business Income Coverage** - If your business is unable to operate due to a cyber breach of your network or the network of your cloud service provider, this coverage provides business interruption coverage.

- **Cyber Extortion Threat** – Cyber extortionists may threaten to harm you, your reputation, or your property if you do not comply with their demands.
  Cyber extortion can take many forms. For example, the cybercriminal may use "ransomware" to encrypt your data, which means you can't read your data without the encryption key – and the cybercriminal will withhold this key until payment is made. This coverage is needed for situations where you must make a payment to eliminate credible threats.

- **Cyber-Theft Loss** – Cyber-attacks are now more sophisticated than ever before. This coverage will reimburse your company for the loss of money due to the unauthorized transfer of funds, service credits or tangible property.

- **Cyber-Fraud Event** – This occurs when a criminal enterprise disguises themselves as an employee, client or vendor and tricks someone at your organization into transferring funds to an account under their control. This could come from a phishing attack or social engineering email, text or instant message.

- **PCI DSS Assessment Coverage** – Did you know that businesses are required to implement a set of security standards to protect credit card data? This insuring agreement provides coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.