## Cyber Liability Coverage History: Theft of Data

- Identity Theft: In the past, Cyber Crime was typically associated with the acquisition of the personal data of large groups of people. With that personal data, the criminals could take over the identity of others so that they could fraudulently obtain loans or get credit cards.

- Laws have been established to hold businesses liable if personal data was taken from their systems, and these laws require that the business owners
  - Determine the extent of the data breach,
  - Notify those whose data was breached, and
  - Pay to monitor the credit of those impacted.

- The standard General Liability policy does not cover this type of exposure because it only covers Bodily Injury and Property Damage caused by your business products or operations to a 3rd party.

Because "Cyber" attacks on businesses are becoming more prevalent, insurance carriers have started to add endorsements to pick up business owners' "Liability" exposures for a cyber-attack / data breach.

These offerings most commonly come as an endorsement attached to the General Liability policy, but most carriers offer "stand alone" Cyber Liability policies.

- These first wave of "Cyber Liability" policies typically address
  - Forensic Services (to determine when / how / what data was compromised),
  - Notification expenses (for those whose data was compromised),
  - Call Center Costs,
  - Legal Services, and
  - Identity Monitoring.

- These coverage forms vary from carrier to carrier and are often restricted to a limit of $5,000 or $10,000 per occurrence.

To purchase a higher limit, a business will need go through an underwriting process to purchase a separate "Cyber" policy.

## What we are seeing in 2018: The Theft of Money / Crime Covg.

The focus of Cyber Attacks has shifted.

- Cyber Criminals can now take over your computer system and hold your systems and data "hostage". They demand a ransom for the return of access to your system. This is called "Cyber Extortion".

- Cyber Criminals are watching your email exchanges with your banks. They monitor your accounts payable and accounts receivable, and they interject themselves into the process to take your money. This is called "Fraudulent Funds Transfer".

Not all carriers offer coverage for Fraudulent Funds Transfer or Cyber Extortion, but many carriers now offer one or both coverages as part of their Cyber Coverage Option.

**EXAMPLE:**

# Philadelphia Insurance Co.

## CYBER LIABILITY

COVERAGE SYNOPSIS

Our Cyber Liability Insuring Agreements are **offered on an "á la carte" basis** whereby your insured can pick and choose which coverage parts they would like to purchase and their associated premiums. Your client can opt for all Coverage Limits we are offering or they can select just a single part to complement their existing risk management program.

### Philadelphia Insurance Cyber Liability Insuring Agreements

**A. Loss of Digital Assets**: Loss you incur as direct result of damage, alteration, corruption, distortion, theft, misuse or destruction of electronic data and computer programs.

**B. Non-Physical Business Interruption and Extra Expense**: Reimbursement for income loss, interruption expenses, and special expenses as a result of the total or partial interruption, degradation in service, or failure of the computer system.

**C. Cyber Extortion Threat**: Reimbursement for the extortion expenses and extortion monies resulting directly from a credible threat or series of threats.

**D. Security Event Costs** *(Your own direct costs for a privacy breach, security breach or breach of your privacy policy):* Reimbursement for security event costs such as notification costs, computer forensic costs and credit protection services. This also includes costs incurred to minimize harm to your brand or reputation, regulatory fines and penalties (where insurable) and any monies required for a Consumer Redress Fund.

**E. Network Security and Privacy Liability Coverage** *(legal liability for a cyber event):* Payment on your behalf which you are obligated to pay as damages and claims expenses from your acts, errors or omissions or for others for which you are responsible including outsourcers and vendors following a security breach or privacy breach.

**F. Employee Privacy Liability Coverage** *(legal liability for breach of employee's PII or PHI):* Payment on your behalf in which you are obligated to pay as damages and claims expenses arising out of a privacy breach involving an employee's private information.

**G. Electronic Media Liability Coverage**: Payment on your behalf for damages and claims expenses as a result of

a. defamation, libel and slander
b. invasion of an individual's right of privacy of publicity
c. plagiarism or misappropriation of ideas under an implied contract
d. infringement of any copyright, trademark, title, service mark
e. domain name infringement or improper deep-linking or framing

**H. Cyber Terrorism Coverage**: Reimbursement for income loss, interruption expenses and special expenses directly as a result of total or partial interruption, degradation in service, or failure of the computer system which is directly caused by an act of terrorism.

**Note: Fraudulent Funds Transfer is not covered.**

## "Take Aways"

- Make sure that you know what is and is NOT included in your Cyber Coverage Policy.
- Ask your agent to compare quotes from at least 2 insurance companies.

**A good policy should cover**

**- Forensic Services** (to determine when / how / what data was compromised),

**- Notification Expenses** (for those whose data was compromised),

**- Credit Protection Services**,

**- Regulatory Fines and Penalties,**

**- Legal Defense Services**,

**- Identity Monitoring,**

**- Cyber Crime (loss of $ assets)**
**Fraudulent Funds Transfer**
**Cyber Extortion.**

- Coverage for **Loss of Income & Extra Expense**

## Ask Yourself:

How much do you have to lose?????

- What is your largest receivable?
- How much is your largest payable?
- How much is in your bank accounts?

---

Feel free to contact me for any questions or to look at coverage options.

**Herb Phelps, CIC**
**Network Insurance Services, LLC**
5261 S. Quebec St., Suite 100
Greenwood Village, CO 80111
**Direct: 303-705-9883**
Fax: 303-708-0202
**Email: herbp@thinknis.com**