There is far more coverage in a cyber policy than for just the theft of credit card information. Just a few examples include:

-If you collect or store any PII or PHI of customers or employees in any format, you are vulnerable to a breach. A well written cyber policy covers the cost to notify and provide credit monitoring services to those affected.

-If you rely upon a computer to conduct your business operations, a virus, malware or cyber extortion event could cause a loss of your ability to access information and continue operations, resulting in a loss of business revenues. This coverage is available with most cyber insurers.

-If a virus, malware or a hacker damages or destroys your database, your cyber policy may help cover the cost to restore your systems to the state they were in prior to the attack.

-If you store important data on your computer and it is connected to the internet, you could become a victim of cyber extortion, including ransomware. Cyber policies can cover the ransom demand to regain control of your data, or the cost to rebuild the database, and to restore the data from backup files.

-If you post any content on your website or other social media, a cyber policy can help defend you in the event of an intellectual property claim.

-If you transfer funds electronically, you may fall victim to a social engineering scam, which may be covered under your cyber policy.

-If you become a victim of any of the perils insured under a cyber policy, one of the primary benefits of that policy is to have an experienced partner to manage the situation. While your organization may have never experienced a breach, a qualified cyber insurance carrier has likely handled several situations like yours before.

- The best carriers will provide you with a breach coach to assist you in managing a data breach.
- Most cyber carriers will have pre-negotiated rates with vetted vendors which can save you money and time in handling the breach