

## 1. How does PCI Compliance affect Cyber Liability?

A Cyber Liability policy will not respond to a breach, where credit card information is compromised, if the entity in question is not PCI (Payment Card Industry) compliant. The Payment Card Industry Data Security Standard is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.

There are six main requirements for PCI compliance. The vendor must:

1. Build and maintain a secure network:
  - Install and maintain a firewall configuration to protect cardholder data.
  - Not use vendor supplied defaults for system passwords and other security parameters.
2. Protect cardholder data:
  - Protect stored cardholder data.
  - Encrypt transmission of cardholder data across open, public networks.
3. Maintain a vulnerability management program:
  - Use and regularly update anti-virus software.
  - Develop and maintain secure systems and applications.
4. Implement strong access control measures:
  - Restrict access to cardholder data by business need-to-know.
  - Assign a unique ID to each person with computer access.
  - Restrict physical access to cardholder data.
5. Regularly monitor and test networks:
  - Track and monitor all access to network resources and cardholder data.
  - Regularly test security systems and processes.
6. Maintain an information security policy:
  - Maintain a policy that addresses information security.

## 2. Is it necessary to get Fidelity Bond Coverage as well as Crime Coverage?

A fidelity bond covers employee theft/fraud exposures only. A crime policy includes not only Employee Dishonesty coverage, but can also cover Forgery and Alteration, Theft of Money and Securities, Robbery and/or Burglary of a Safe, Computer Fraud & Funds Transfer Fraud.

## 3. Doesn't Employment Practices have different insurance than D&O?

They cover different exposures. A Directors & Officers policy covers the exposure of the Directors and Officers and their duties of loyalty, care and obedience to the organization. An Employment Practices Liability policy covers harassment and discrimination in the workplace, wrongful firing and wrongful hiring practices. Employment Practices Liability coverage can be a standalone policy or a component of a Directors & Officers policy.

**4. With regard to Cyber Liability, if we don't store credit card numbers or Social Security numbers and our data base simply holds names and addresses, is coverage needed?**

If you do not also have any of the following exposures, it certainly reduces your exposure:

- Patient health information
- Date of birth information
- Customer user name and passwords
- Customer or employee contact information
- Financial records and account information
- Driver's license number

However, any information that is compromised can lead to litigation but certainly the lower the exposure, the lower the cost of coverage.