Myth: I'm a small merchant who only takes a handful of cards, so I don't need PCI.
Fact: This is a common misunderstanding with the standard, that small merchants handling only one or a few credit cards a year are exempt from compliance. If you are a merchant and are set up to take credit cards by any mechanism - then you need to be complaint.

Myth: PCI only applies to e-commerce companies.
Fact: No, PCI applies to every company that stores, processes or transmits cardholder information. In fact anyone who takes card present transactions that involve POS devices are typically more at risk than e-commerce solutions. Quite often these types of transactions involve storage of track data (which is forbidden under PCI). Compromise of this type of data may bring heavy fines and requests for compensation from the banks involved.

Myth: You only have to be PCI compliant with the majority of criteria.
Fact: The pass mark for PCI is 100%, so if you fail even one of the criteria, you are not PCI compliant. The standard is not meant to be something to strive for; it is essentially a floor, a basis for further security measures. Failing to achieve even one of the requirements, is failing to meet a basic standard for handling cardholder information. All companies that routinely handle this type of data should be aiming to exceed the standard. It's just good business.

Myth: I only need to protect my credit card data, not ATM debit card related data.
Fact: Incorrect - both are required. Many debit cards are dual-purpose 'signature debit', which can be used on debit and credit card networks. As such, they are covered under PCI and must be protected in the same way as credit cards.

Myth: I can wait until my business grows.
Fact: Incorrect - the PCI standard applies to all sizes of business and waiting could be costly. Should you be compromised and not be PCI compliant, the fines and the compensation requirements by the banks (it typically costs between $50 and $90 to replace one card) could be substantial.

Myth: I can just answer 'yes' to all the criteria on the Self-Assessment Questionnaire (SAQ).
Fact: The Self-Assessment Questionnaire (SAQ) is a mechanism for getting the information about the level of your compliance to your merchant bank. The standard applies at all times. Just saying yes to the questions puts you at great risk. If a compromise took place and it was obvious that you were not and have never been PCI compliant, the matter would be taken very seriously. You would be risking your whole business by answering 'yes' to the questions, when there is no factual basis for the answers.

Myth: I can wait until my bank asks me to be PCI compliant.
Fact: The dates for merchants to be PCI compliant are long gone. You are responsible for making sure you are in compliance. Waiting until the bank asks you could be very costly indeed.

Fact: The PCI standard forms part of the operating regulations that are the rules under which merchants are allowed to operate merchant accounts. The regulations signed when you open an account at the bank state that the VISA regulations have to be adhered to. Even if you have been in business for decades, PCI still applies if you store, process or transmit credit cards.

Myth: As a merchant, I'm entitled to store any data.
Fact: Many merchants believe that they own the customer and have a right to store all the data about that customer in order to help their business. Not only is this incorrect regarding PCI, it may also be a violation of State and Federal legislation regarding privacy. The PCI regulations specifically forbid storing of any of the following:

1. **Unencrypted credit card number**
2. **CVV or CVV2**
3. **Pin blocks**
4. **PIN numbers**
5. **Track 1 or 2 data**

Any of the above found in databases, log files, audit trails, backup's etc. can result in serious consequences for the merchant, especially if a compromise has taken place.

Myth: One vendor and product will make us compliant.
Fact: Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. When marketing focuses on one product's capabilities and excludes positioning these with other requirements of PCI DSS, the resulting perception of a 'silver bullet' might lead some to believe that the point product provides 'compliance', when it's really implementing just one or a few pieces of the standard. The PCI Security Standards Council urges merchants and processors to avoid focusing on point products for PCI security and compliance. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the 'big picture' related to the intent of PCI DSS requirements.

Myth: Outsourcing card processing makes us compliant.
Fact: Outsourcing simplifies payment card processing but does not provide automatic compliance. Don't forget to address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process charge backs and refunds. You must also ensure that providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data. You should request a certificate of compliance annually from providers.

Myth: PCI compliance is an IT project.
Fact: The IT staff implements technical and operational aspects of PCI-related systems, but compliance to the payment brand's programs is much more than a 'project' with a beginning and end – it's an ongoing process of assessment, remediation and reporting. PCI compliance is a business issue that is best addressed by a multi-disciplinary team. The risks of compromise are financial and reputational, so they affect the whole organization. Be sure your business addresses policies and procedures as they apply to the entire card payment acceptance and processing workflow.

Myth: PCI will make us secure.
Fact: Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

Myth: PCI is unreasonable; it requires too much.
Fact: Most aspects of the PCI DSS are already a common best practice for security. The standard also permits the option using compensating controls to meet some requirements. The standard provides significant detail, which benefits merchants and processors by not leaving them to wonder, 'Where do I go from here?' This scope and flexibility leads some to view PCI DSS as an effective standard for securing all sensitive information.

Myth: PCI requires us to hire a Qualified Security Assessor (QSA).
Fact: Because most large merchants have complex IT environments, many hire a QSA to glean their specialized value for on-site security assessments required by PCI DSS. The QSA also makes it easier to develop and get approval for a compensating control. However, PCI DSS provides the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. Mid-sized and smaller merchants may use the Self-Assessment Questionnaire (SAQ) found on the PCI SSC Website to assess themselves.

Myth: PCI makes us store cardholder data.
Fact: Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card. If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable.

Myth: PCI is too hard.
Fact: Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for merchants without security or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyways to protect sensitive data and continuity of operations. There are many products and services available to help meet the requirements for security – and PCI compliance. When people say PCI is too hard, many really mean to say compliance is not cheap. The business risks and ultimate costs of non-compliance, however, can vastly exceed implementing PCI DSS – such as fines, legal fees, decreases in stock equity, and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.