

Toronto / Washington DC / Brussels
www.nymity.com



Chris Zoladz

Founder
Navigate LLC

Why PCI Compliance Is So Confusing: You Too Can Take Charge!

PCI is something you often hear about when there is some form of media event or you get a notice from your financial institution requiring that you comply. In both situations, many of us lack the technical knowledge to understand how to lower our risks and costs and effectively take action.

Chris Zoladz, Founder of Navigate LLC, provides us with meaningful information to help our clients or ourselves not only understand what PCI is, but also, to know if it applies to us, our risks of non-compliance, where we can get implementation advice, and how to keep current with changing requirements.

Chris has been heavily involved in PCI compliance efforts since the standard was first published in 2006 and before PCI when the credit card brands maintained their own standards (e.g., Visa's Cardholder Information Security Program or CISP). His experience includes multi-year PCI compliance efforts at two large international companies as well as consulting with smaller organizations.

To help make PCI understandable and actionable for small and medium companies without emptying their bank account, Navigate has created a monthly subscription e-publication called The PCI Coach (www.thepcicoach.com).

Nymity: What is PCI?

Zoladz: PCI stands for the "Payment Card Industry" and is the abbreviation for the "Payment Card Industry Data Security Standard" or "PCI DSS." PCI is a set of approximately 225 technical and business detailed process requirements included in the following 12 high level categories:

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security policy

The PCI requirements must be satisfied for every system, computing infrastructure component and business process that involves the collection, processing, storage or transmission of credit card data. PCI is very comprehensive and is a global standard. The PCI standard is maintained by the PCI Security Standards Council (www.pcisecuritystandardscouncil.com), an entity created by the major credit card companies several years ago.

Nymity: Who must comply?

Zoladz: Basically, any business (referred to as merchants) that collects, processes, transmits or stores credit cards is obligated to comply. Service providers, such as those that provide on-line shopping cart services and banks are also subject to PCI. It is a company's responsibility to select only PCI compliant service providers and software products when credit card data is involved.

Nymity: Why is it difficult and confusing, especially for small and medium businesses to comply?

Zoladz: Most small businesses generally do not have an IT or compliance staff and medium size businesses may have only minimal IT staff that are consumed with day-to-day needs. As a result, there are no internal resources to analyze the PCI requirements, some of which are not straightforward and many others are highly technical and it is difficult to understand how they apply to the business, and how to most cost-effectively achieve compliance. This reality coupled with one of the toughest business environments in years makes it very tempting to push aside PCI compliance for other priorities, especially if your merchant bank¹ is not pressuring you to become compliant.

Nymity: What are the risks and liabilities of non-compliance?

Zoladz: The greatest risk is that a company's credit card data may not be adequately protected. If this data is lost or stolen and credit card fraud occurs, the company's customers will not be pleased, and the company will likely suffer at least some loss of customer loyalty. In addition, the credit card companies can require a forensic review at your expense, levy fines through your merchant bank if your company is not PCI compliant and also seek recovery of the fraudulent charges that were committed on the lost or stolen credit card data. Lastly, if there is lost or stolen credit card data, there are 46 State security breach laws that may require you to notify the affected individuals and the State Attorney General in certain states. Addressing these requirements can be costly as notification letters will need to be printed and mailed, the expected offering of at least one year of complimentary credit monitoring service is procured, and legal counsel advice is obtained. In summary, the stakes and consequences of non-compliance can be very high.

Nymity: What free resources are available to help companies?

Zoladz: The PCI Security Standards Council has an abundance of helpful materials on their website. It can sometimes be bit challenging to navigate the website so be persistent. However, keep in mind that "the PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards." As such, the Council does not take a position on how to achieve compliance or on specific products or software vendors. There are also free vendor webinars and seminars but these events tend to focus on the product or service of the sponsor.

Nymity: What options are available to help companies comply?

Zoladz: As with any compliance effort, there is the do-it-yourself approach using all internal resources, using a consultant, or a combination of internal resources teamed with a consultant. The most effective approach is specific to the company. For example, a small family owned business with three restaurants that uses an IT service provider to install and maintain the computers and systems used at the restaurants will likely need to use a consultant to help them achieve PCI compliance. However, the budgets for consulting services may be limited. For this reason, companies like Navigate have created tools to help, such as our monthly subscription e-publication called The PCI Coach (www.thepcicoach.com) to help make PCI understandable and actionable for these companies without emptying their bank account.

Nymity: What can companies do to reduce their costs and yet increase their compliance status?

Zoladz: The most impactful action any company can take is to review and challenge their current business practices and determine if there is any way to reduce the number of systems and business processes that involve credit card data without adversely impacting the business. If changes can be made so credit card data is in fewer places, the scope and cost of compliance can be immediately reduced. For example, I have observed some hotels that still make a physical imprint of a credit card and also enter swipe the card into an automated system for authorization and transmission of charges. In this case, the paper record of the card data serves no

¹ Also referred to as the "acquirer" is the intermediary that facilitates the charging of the credit card and payment to the merchant. The merchant bank is also the intermediary between the merchant and the credit card companies as it relates to enforcing PCI compliance and any associated non-compliance penalties.

necessary purpose, is redundant to the electronic record and the merchant then has the burden of protecting the redundant paper record. So, discontinuing the practice of making credit card imprints will reduce scope. A more profound example, would be questioning whether the use of a point of sale system to submit credit card transactions is really necessary. For a small company, the number of credit card transactions may be small enough that using a \$300 bank terminal that communicates to the bank via a telephone line meets the business needs. If it does, avoiding putting credit card data in the point of sale systems eliminates the need to ensure a compliant version of the point of system is in place (and any related system upgrades) and the network it resides on meet all the PCI requirements, all of which can be costly.

Nymity: Where does a company typically start?

Zoladz: The first activity that needs to be completed is an inventory of all the places that credit card data is collected, processed, stored and transmitted, including third party service providers. A company cannot accurately scope their PCI compliance effort and create a holistic compliance strategy until this inventory is completed.

Another key activity is to review the Self-Assessment Questionnaire (SAQ) published by the PCI Security Standards Council. By doing this a company will have a better understanding of what they will need to do and what skills they will need to acquire for help. For example, the first PCI requirement addressing firewalls is technical. Would you have the necessary resources to establish firewall and router configuration standards that include requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone? Or how about building a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment? These examples illustrate how compliance can be complex for small and medium size business that do not have the necessary in-house IT expertise.

Nymity: How does a company know if it is compliant?

Zoladz: An independent assessment by a PCI Qualified Security Assessor (QSA) is arguably the most effective validation. In fact, for larger merchants (referred to as Level 1 or 2) an annual review by a QSA is required. A company can also complete a self-assessment using the Self-Assessment Questionnaire (SAQ) published by the PCI Security Standards Council. Smaller merchants (Level 3 and 4) are required to complete a SAQ on an annual basis. From a compliance monitoring perspective, an independent review vs. self-assessment is the difference between large and small merchants.

Nymity: What is the most important issue a company should know about PCI?

Zoladz: Do not underestimate the level of effort to ensure that the many technical and business process requirements are compliant. To achieve PCI compliance requires an investment of time and financial resources, however, it is achievable.

Nymity: In closing is there anything that you would like to share with our readers that we have not asked?

Zoladz: PCI compliance should be taken seriously by businesses of all sizes and you should remember that the credit card companies expect that your company is already compliant. It is easy to ignore or defer PCI compliance efforts if your merchant bank has not asked about your state of compliance or has not been forceful in encouraging compliance by assessing monthly fines. However, ignoring PCI compliance would be a mistake. Eventually, your company will be accountable for your PCI compliance and it can be easier and more effective to work toward compliance before you are asked about your status or forced to comply in a short period time. My best advice is to create a realistic compliance strategy and do as much as you can as fast as you can.