Teaching Case
Do you take credit cards? Security and compliance for the credit card payment industry

Lorrie Willey
Barbara Jo White
Business Administration and Law
Computer Information Systems
Western Carolina University
Cullowhee, NC 28723, USA
lwilley@email.wcu.edu, whiteb@email.wcu.edu

ABSTRACT

Security is a significant concern in business and in information systems (IS) education from both a technological and a strategic standpoint. Students can benefit from the study of information systems security when security concepts are introduced in the context of real-world industry standards. The development of a data security standard for organizations operating within the credit card payment industry serves as an excellent example of a real-world security standard that lends itself to classroom study. The establishment and requirements of the Payment Card Industry Data Security Standard (PCI DSS), and the associated consequences for noncompliance, represents a businesslike approach to the organizational protection of data that students will find interesting and one to which they will relate. Everybody uses credit cards! Incorporating the topic of PCI DSS into an activity allows students to learn and apply PCI DSS concepts to a business setting. Just asking "If everyone uses credit cards, why don't all businesses accept them?" will start a process of exploration for the class. A hypothetical business teaching case, *Blue Mountain Jams* (*BMJ*), illustrates the challenge of PCI DSS mandates for small businesses. Small business is given some leeway in self-assessment under PCI DSS to document compliance after the decision is made to accept credit card payments. That leeway gives students the opportunity to learn and analyze the PCI DSS requirements and compliance methods and to determine the best course of action for a business that has made the decision to start accepting credit cards.

Keywords: Critical thinking, Information assurance and security, Security, Teaching Case

1. INTRODUCTION

CIOs participating in Gartner's annual survey ranked security technologies as a top-ten technology priority nearly every year since 2005 (Gartner, 2005; Gartner, 2006; Gartner, 2007; Gartner, 2008; Gartner, 2009; Gartner, 2010; Gartner, 2012; Gartner, 2013). What's more, considering business priorities, improving business continuity, risk and security was a top-ten priority in 2011 (Gartner, 2011) and security breaches and disruptions were top-ten business priorities in 2005 and 2006 (Gartner, 2005; Gartner, 2006). No doubt, some of their security concerns include credit card use. Recently, Global Payments, a credit card payment processor, reported the concern that up to 1.5 million card numbers had been accessed by hackers (Pepitone, 2012).

Despite data breaches, consumers are not dissuaded from acquiring and using credit cards. Estimates place the number of credit cards in the United States (U.S.) at 609 million and the volume of credit card purchases in 2011 at $2.1 trillion. (2012 US Credit Cards Usage Statistics, n.d.). It may come as a surprise to consumers, and to students, however, that many retailers don't accept credit cards. In fact, a survey of small businesses, defined as those with fewer than 250 employees, showed that under half accept credit cards (Dennis & William, 2008). One reason businesses don't accept credit cards may involve the perceptions that complying with credit card security requirements is both complicated and costly.

There is no doubt that students in information systems classes need to have a firm understanding of security requirements faced by businesses, large and small, and the negative consequences of business noncompliance. This knowledge, according to the 2009 White House Cyberspace Policy Review, can "help organizations… make smart choices as they manage risk" (p.13). Students already understand the subject of credit card purchases through personal experiences and the PCI DSS standard makes for an accessible class activity involving data security.

Simultaneously, the teaching case provides an opportunity to better understand PCI DSS and ways by which small businesses can meet those security requirements.

2. *BLUE MOUNTAIN JAMS* SCENARIO

"Do you take credit cards?" the customer asked. That was a question the owners of *Blue Mountain Jams* were being asked over and over.

Mary smiled, "Not yet but we are working on it. Hopefully, staring next month, we will." Once again, Mary wondered how much business they lost because they did not take credit cards. With the business growing, more and more people ask about paying by credit cards. *BMJ* is losing customers by not having that payment option.

Located in the Blue Ridge Mountains of North Carolina, *BMJ* recording studio and retail store is the life ambition of the owners, John and Mary. Graduates of a local university with degrees in music and business, John and Mary have played the bluegrass scene in Western North Carolina and especially Asheville, since their high school years. The success of the company is being inhibited by the need for customers to pay with cash or check.

"John, that's another customer asking about credit cards," Mary said once the shop emptied out. "We have got to deal with this now." John nodded in agreement.

The thought of taking on another major project for the business was intimidating. Starting the studio was an expensive and exhausting enterprise; acting as both musicians and business owners is demanding. John and Mary struggled to raise the funds to get the venture started and they knew that the step to credit cards was necessary to take the business to the next level. There is no question of *BMJ's* success; John and Mary's music knowledge and contacts in the local bluegrass music scene allows for the development of an extensive repertoire of country and bluegrass music. As well, *BMJ* has a positive reputation for preserving the traditional music of the mountains. Critical acclaim and financial success is great but not accepting credit cards is holding the business back. Like most small business owners, accepting credit cards was a step into the unknown.

"I remember from an IS class that there are data security issues we would have to deal with and I am just not sure if our computer systems are set up for credit cards," John replied. "Karen next door told me that the credit card company had all sorts of security requirements and I have no idea what those policies are or how we can start the process for our business and employees. On top of that, she told me there is some crazy self-assessment we would have to do and she said it was way beyond her. Is accepting credit cards worth it? I guess it is time to find out."

Later than afternoon, and feeling somewhat overwhelmed with the project, John calls a local business, *Technology Solutions*, the business for which your students work. After discussing his ideas with the boss, your students are assigned the task of uncovering the information John needs to answer his concerns and get *BMJ* answering "Do you take credit cards?" in the affirmative.

3. SECURITY IN THE INFORMATION SYSTEMS (IS) CURRICULUM

Security has long been part of the undergraduate-level information systems curriculum. In fact, security topics appeared in six of the nine courses in the 1997 model curriculum guidelines for IS undergraduate education, the first produced by the collaboration between the Association for Computing Machinery (ACM) and the Association of Information Systems (AIS), along with the Association for Information Technology Professionals (Davis, Gorgone, Couger, Feinstein, & Longenecker, 1997). There was not a major revision to the guidelines for over a decade, although there was a minor revision in 2002, to reflect the growing interest and impact of e-commerce and a course, *Electronic Business Strategy, Architecture and Design* was recommended to be included in the ten-course curriculum, and a previous course, productivity tools, moved to prerequisite status (Gorgone, Davis, Valacich, Topi, Feinstein, & Longenecker, 2002).

The 2010 revision of the model curriculum guidelines, which removed the e-commerce course from the core, shows a much greater emphasis on security and information assurance and compliance (Topi, Valacich, Wright, Kaiser, Nunamaker, Sipior, & de Vreede, 2010). For example, the term *security* appears eight times in the 2002 model curriculum guidelines and the terms *assurance* or *compliance* appear two times (Gorgone, et al, 2002). However, in the 2010 curriculum guidelines, the terms *assurance* or *compliance* appear six times while *security* appears 49 times (Topi et al., 2010). Although information assurance, compliance and security showed major changes from 2002 to 2010, with securing data and infrastructure along with the need to understand, manage and control IT risks considered high-level capabilities for IS students in 2010, other important skills showed no changes. For example, strong analytical skills, critical thinking skills and communication skills have been integral to IS model curriculum guidelines for over 15 years (Davis et al., 1997, Gorgone et al., 2002, Topi et al., 2010). It is important that class exercises and teaching cases address these types of curriculum needs while promoting active and engaged learning (Willey, Ford, White, & Clapper, 2011).

4. RETAIL PAYMENT AND THE DEVELOPMENT OF PCI DSS

Students can start their analysis of *BMJ* and its credit card security concerns with an overview of the development of the global PCI DSS for the retail payment industry.

4.1 Retail payment system

The credit card industry uses two methods to effect payment: a unitary system and a distributed system. American Express and Discover use the unitary system, promoting the use of their cards directly to merchants and consumers. Visa and MasterCard, on the other hand, use a three-party distributed system, in which a merchant bank issues credit cards to consumers on behalf of Visa or MasterCard and also works with merchants (MacCarthy, 2012).

Regardless of the method, the information required to authenticate face-to-face credit card transactions in the U.S. is embedded in each credit card's magnetic stripe. The account number acts as a routing mechanism across the payment network to direct the charge information to the merchant bank. An embedded security code, called the card verification value (CVV) serves as an authenticating access code allowing the merchant bank to accept or decline the charge. Without the account number and CVV, the merchant bank will not authorize the charge (MacCarthy, 2012).

4.2 PCI DSS development

The development of PCI DSS in 2004 by American Express, Visa, MasterCard, Discover and JCB established industry-wide requirements for credit card payment security. This industry standard replaces individual efforts of credit cards companies to contractually establish security protocols between banks and merchants (Morse & Raval, 2012). The focus of the standard is to eliminate the storage of the magnetic stripe information, the account number and the CVV, on computers within the payment network (MacCarthy, 2011). The oversight board, the Payment Card Industry Council (PCI Council), established in 2006, allows all participants in the credit card retail payment industry to be involved in the development of standards (Frye, 2006). The Council drafts rules, provides guidance and initiates programs for to assure compliance (Messmer, 2012).

Any entity, such as a merchant or merchant bank, along the payment network, regardless of size or number of transactions, storing data in violation of the PCI DSS standards allows for vulnerability throughout the system. Storing the account number and CVV is not only unnecessary but allows hackers to access the information and sell it for fraudulent use, the most common of which is the creation of counterfeit cards (MacCarthy, 2011). "Thieves can clone it onto another piece of plastic in a matter of seconds, a use it for hundreds of transactions" (Segal, Ngugi & Manna, 2011, p. 760).

With the institution of PCI DSS, the Council claims that compliance has decreased the number of data theft instances. At its 2012 European Community meeting, the council claimed that "we don't see the massive data breaches that we used to" ("Fewer thefts of credit card data," 2012).

4.4 PCI DSS and retail payment abroad

Although PCI DSS sets the bar for all retail credit card payment security, the system is not a guarantee. Since the account number and CVV can be hacked if improperly stored or even while in transit, having all the information necessary to create and use counterfeit cards available in the magnetic stripe of a credit card is considered by some, specifically members of the international community, to be a security risk. In the U. S., "[t]he problem is that credit card companies are wedded to a fraud-prone technology: credit cards with magnetic stripes" (Segal et al., 2011, p. 760).

The European Union addressed this security concern by adopting smartcards for credit transactions which require the use of a personal identification number (PIN). Under this system, the magnetic stripe contains the account number but the consumer must key a PIN into the system. A microprocessor, the chip, transmits encrypted information when used with a terminal able to generate and receive the information. The interaction between smartcard and terminal results in the transmission of an authorization code that is different with each use of the smartcard. Therefore, even if card information is stored, the information is useless to hackers (MacCarthy, 2012).

As a result of the adoption of chip and PIN, credit card fraud in face-to-face transactions the United Kingdom, went from £214.8 million in 2004 to £72.1 million in 2009 (MacCarthy, 2011). France saw a 78% drop in credit card fraud in the first year after adopting chip and PIN technology in 1993 (Segal et al., 2011).

From a global perspective, the concern that continued usage of the magnetic stripe with account number and CVV is straightforward; the "financial services world is an interconnected system. "Vulnerabilities at one point affect other nodes in the system" (MacCarthy, 2012, p. 269). As for the United States, "The U.S. is being blown away by security investments overseas, and our 1950s-era system is making us the weak link in the security chain" (Congressional Hearings, 2009, p. 3).

5. CURRENT PCI DSS REQUIREMENTS AND COMPLIANCE

With a clearer idea of what the owners of *BMJ* are taking on with the decision to accept credit card payments, students are now ready to consider the specific requirements of the data security standard. Similar to concepts introduced when discussing data security in any organization, the requirements provide not only PCI DSS specifics, but a broader awareness of the nature of data security standards for all organizations ("Payment Card Industry," 2010).

The current version of the PCI DSS (version 2) requirements consist of six broad objectives: build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. From protection of sensitive data from those with criminal intent, to the establishment of policies applicable to maintaining data securely, the PCI DSS objectives and requirements, identified below in Table 1 (on the following page), provide guidance to business implementing the compliance process.

5.1 Current PCI DSS Requirements

While businesses may have difficulty understanding PCI DSS requirements, information systems students, on the other hand, will find the requirements direct and easy to understand. The storage of cardholder data is the essential concern and under the requirements that data should not be stored except when mandatory for business needs. Even then, any information stored must be at a minimum and purged when no longer needed. Not difficult concepts, but they do entail a broad array of analysis and activities within an organization. A merchant's failure to change the default passwords used in its point of sale system, for example, can result in noncompliance with PCI DSS since vendor-supplied defaults must be changed before any system is added to the network. Techniques to ensure PCI DSS compliance will be familiar to IS students.

5.2 PCI DSS Compliance

A recent study of business compliance with PCI DSS requirements showed that businesses find some requirements more difficult to comply with compared to others ("Verizon 2011 PCI Compliance Report," 2011).

Table 1. Current PCI DSS Requirements* and Rates of Compliance**

PCI Objective*	PCI DSS Requirement*	08-'09**	2010**
Build and Maintain a Secure Network	**Requirement 1**. Install and maintain a firewall configuration to protect cardholder data	46%	44%
	Requirement 2. Do not use vendor-supplied defaults for system passwords and other security parameters	48%	56%
Protect Cardholder Data	**Requirement 3**. Protect stored cardholder data	43%	42%
	Requirement 4. Encrypt transmission of cardholder data and sensitive information across open, public networks	63%	72%
Maintain a Vulnerability Management Program	**Requirement 5**. Use and regularly update anti-virus software or programs	70%	64%
	Requirement 6. Develop and maintain secure systems and applications	48%	53%
Implement Strong Access Control Measures	**Requirement 7**. Restrict access to cardholder data by business need-to-know	69%	75%
	Requirement 8. Assign a unique ID to each person with computer access	44%	47%
	Requirement 9. Restrict physical access to cardholder data	59%	55%
Regularly Monitor and Test Networks	**Requirement 10**. Track and monitor all access to network resources and cardholder data	39%	52%
	Requirement 11. Regularly test security systems and processes	38%	37%
Maintain an Information Security Policy	**Requirement 12**. Maintain a policy that addresses information security for all personnel	44%	39%

* *Note*. From "PCI DSS Requirements and Security Assessment Procedures, version 2.0" by PCI Security Standards Council, LLC, 2010, p. 5.

** *Note*. From "Verizon 2011 Payment Card Industry Compliance Report" by The Verizon PCI and RISK Intelligence Teams, 2011, p. 10.

For example, businesses found the following four requirements most difficult to implement: protecting cardholder data (requirement 3); tracking and monitoring access (requirement 10); testing systems and processes on a regular basis (requirement 11), and maintaining security policies (requirement 12). On average, across both study years, the rate of compliance was less than 43%, On the other hand, businesses found it easier to implement the following PCI DSS requirements: encrypting transmissions over public networks (requirement 4); using and updating anti-virus software (requirement 5); restricting access to a need-to-know basis (requirement 7) and restricting physical access (requirement 9). On average, for the four requirements above, the rate of compliance was above 65%.

PCI DSS compliance is required under contractual agreement by all parties within the payment process. Under the contract terms, merchant banks require merchants to be PCI DSS compliant and to verify compliance annually (Segal et al., 2011). Large merchants, those with over six million transactions annually, are required to utilize independent auditors to ensure compliance; small merchants, those with up to twenty thousand annual transactions, report compliance via self-assessment on a PCI Council-provided questionnaire (Morse & Raval, 2012). As of 2009, 96% of the largest merchants and 94% of the next largest, reported compliance with the standard (MacCarthy, 2011). However, the five million in the smallest merchant category pose a security risk when not in compliance, "…hackers are turning to smaller companies as the larger ones devote more resources to security, and that compliance for small businesses is complex and expensive" ("Global Security Summit," 2009). Recent reports indicate that 90% of all credit card data breaches occur within the confines of small business ("Small merchants make up lion's share," 2011)

Compliance is expensive for large and small merchants. A 2009 National Retail Federation survey estimated member compliance costs at over $1 billion, another estimated compliance costs since 2009 at $2 billion (MacCarthy, 2011). The cost of compliance for small business can reach $81,000.00 (Segal et al., 2011).

5.3 Consequences for noncompliance

Legal liability and associated costs can be extensive when credit card information is breached yet the possibility of a breach remains significant. The 2011 Verizon PCI Compliance Report found only 21% of the survey organizations to be fully compliant with the standards and that in cases of data breach, the organizations involved were likely not to be in compliance. According to the study, protecting stored data, tracking and monitoring access, testing systems and processes and maintaining security policies were the most difficult areas for organizational compliance with the standards ("Verizon 2011 PCI Compliance Report," 2011).

The 2012 Data Breach Investigations Report contains some statistics regarding the means by which breaches occur: external agents were responsible for 98% of total breaches in 2011, 81% involved some form of hacking, and 97% were avoidable by the use of some controls. Small organizations, with 11-100 employees, constituted 570 of the 855 incidents investigated for the report ("2012 Data Breach Investigations," n.d.). The report advises PCI DSS compliance for retailers: "Low levels of PCI DSS adherence highlight a plethora of issues across the board for related organizations" ("2012 Data Breach Investigations," n.d., p. 3).

The costs associated with a breach are allocated by contract between parties within the payment industry which provide that the costs are borne by the financial institution issuing the card whether or not that entity is responsible for the breach (MacCarthy, 2011). These costs include not only in the financial loss from the fraudulent charges, but those associated with notification obligations to consumers, monitoring internal systems for continued fraudulent activity, cancelling and then reissuing new cards for those that have been compromised, and, while not measured in financial terms, the loss of reputation and trust (Rees, 2011).

The federal government also has an interest in data breaches and determining the cause of breaches and imposing sanctions. The Federal Trade Commission Act, which, in part, created the Federal Trade Commission (FTC), provides that the FTC can investigate and take action against companies that engage in unfair and deceptive trade practices (Federal Trade Commission Act, Section 5). Breaches of confidential or personal data, including credit card data, can fall within the realm of unfair and deceptive trade practices. When reviewing credit card breaches, the FTC relies on PCI DSS to determine whether or not the organization has violated law. In essence, the failure of an entity to be PCI DSS compliant is the equivalent to the "failure to employ reasonable and appropriate security measures to protect personal information" (MacCarthy, 2012, p. 253).

Minnesota, Nevada, and Washington have codified PCI DSS requirements to the retail payment industry within their states and allow a civil cause of action against breaching entities that are not PCI DSS compliant when a data breach occurs. Minnesota, for example, allows civil remedies for cost recovery for issuing banks. Recovery includes the costs of cancellation and reissuance of cards, costs incurred when notifying card holders of the breach, as well as the financial loses for unauthorized transactions. The cause of action requires a showing that the breaching merchant maintained card information for more than forty-eight hours (Minn. Stat. Ann, 2007). Nevada requires PCI DSS compliance or encryption for all involving credit card information (Nev. Rev. Stat., 2010).

Should the breaching party be a merchant, not only are state actions or FTC investigations concerns, but ultimately a merchant can be fined, face increased transaction fees or be ousted from the retail payment system, thereby losing the ability to accept credit cards (Rees, 2011).

6. PUTTING IT ALL TOGETHER: BLUE MOUNTAIN JAMS

To ensure accurate verification of compliance, the PCI Council oversees a program that provides training for entities that help merchants with compliance. Qualified Security Assessors (QSAs) are approved by the PCI Council to assess, validate and help report on a merchant's PCI compliance. A merchant would typically hire a QSA as part of its annual compliance process. In reality, only the largest

merchants utilize independent audit ("Become a Qualified Security Assessor," n.d.).

However, for small merchants unable to bear the cost of a SAQ, the PCI Council allows for self-assessment with the use of a SAQ ("PCI DSS Self-Assessment Questionnaire," n.d.). While this represents a significant cost savings, it also requires the merchant to have the technical expertise to understand and correctly fill out the Self-Assessment Questionnaire (SAQ). In fact, since there are a number of different SAQs; an early technical challenge for the merchant is determining which SAQ (A, B, C-VT, C or D) is appropriate for its situation. The number of requirements that must be assessed and reported are significantly different according to the applicable SAQs, as is the cost of completion. Making the decision regarding self-assessment before making the decision to accept credit cards could save a business time and money (Thapar, n.d.).

With the information needed to address the needs of *BMJ*, the *Technology Solutions* team is ready to get to work in deciding the best approach to security compliance for *BMJ*. As the team begins looking at how *BMJ* could accept credit cards, it should become apparent that different approaches are possible, each with its own set of pros and cons. It is clear that small businesses like *BMJ* face challenges in establishing annual compliance and face serious consequences if they do not.

6.1 Which SAQ is the best choice for Blue Mountain Jams?

As a small credit card merchant, *BMJ* must determine which SAQ is appropriate for their compliance reporting. Some SAQs reports require considerably more information than others, so the team begins the process with a detailed comparison of the SAQ's, examining the level of difficulty for completing the questionnaires and identifying the constraints required for the SAQ. All the SAQs can be downloaded by the team at the PCI DSS site ("Documents Library," n.d.).

With the questionnaires in hand, the team will examine each of the SAQs individually, looking at the number of PCI requirements which must be assessed for each SAQ. The more requirements that must be assessed the higher the cost and technological complexity, so *BMJ* would definitely prefer to use an SAQ that would have require fewer PCI requirements. However, each SAQ has a very specific set of conditions that must be met by the merchant in order for them to be able to use that SAQ for their compliance assessment. For example, SAQ A is designed for card-not-present merchants. While it has a low number of PCI requirements, and therefore, would be attractive to *BMJ*, the team will discover that *BMJ* is not eligible to use the SAQ with their current business model.

In the process of trying to find the SAQ that would be most advantageous to their client, the team will utilize their analytical, critical thinking and communication skills (Davis et al., 1997, Gorgone et al., 2002, Topi et al., 2010) as they compare and contrast the SAQs, identify the most attractive, rule out the ones that won't fit with *BMJ* business and communicate their findings to their client. To assist in the analysis, "Instructor Notes" will be provided with a detailed comparison and analysis of the SAQs along with suggestions about which would be the best fit for *BMJ*.

6.2 *Technology Solutions* Report to *BMJ*

After reaching their decision regarding the SAQs, the team reports its findings to the owners of *BMJ*, either in writing or as an oral presentation. The owners of *BMJ* need some general information about PCI DSS requirements and compliance mandates, the seriousness of noncompliance, and the reasoning behind the decision regarding the appropriate SAQ. The report could also include a list of the IS policies needed to establish procedures to maintain security and to train employees on the policies.

6.3 Other tasks related to the *BMJ* scenario

While the SAQ tasks provides a class activity that allows students to read, analyze, critically think and write, there are other activities that can stem from that experience. Ranking and categorizing the PCI DSS security requirements, for example, are easy tasks that allow students to think about the techniques associated with developing and maintain PCI DSS requirements (Willey, White & Stillwell, 2013). Also, there are class discussion opportunities regarding the credit card payment industry move to Chip and PIN. The "Instructor's Notes" contain a variety of PCI DSS activities that can be utilized in the classroom.

7. CONCLUSION

Exposure to the PCI DSS compliance requirements allows students to easily access, engage in, and become familiar with, real-world security issues in the retail payment industry. The topic will be of interest to students and the requirements easy to understand. Data security is not a concern in a vacuum; it comes to life when people and organizations attempt to establish policies and systems necessary to protect information. Working with *BMJ* creates a virtual business experience for students, allowing them to tackle serious issues surrounding the application of industry-specific security requirements in the class-room environment.

8. REFERENCES

2012 Data Breach Investigations Report (n.d.). Retrieved November 17, 2012 from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (2013)

2012 U.S. Credit Card Usage Statistics (n.d.). Retrieved February 8, 2013, from http://visual.ly/2012-us-credit-card-usage-statistics

Become a Qualified Security Assessor (n.d.). Retrieved January 30, 2012 from https://www.pcisecuritystandards.org/approved_companies_providers/become_qsa.php

Congressional Hearings (2009). Do the Payment Card Industry Data Standards Reduce Cybercrime? Retrieved December 11, 2011 from www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/pdf/CHRG-111hhrg52239.pdf

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009).

Retrieved January 9, 2013 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Davis, G. B., Gorgone, J. T., Couger, J. D., Feinstein, D. L., & Longenecker, Jr., H. E. (1997). "IS '97 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems," ACM, New York, NY and AITP [formerly DPMA), Park Ridge, IL.

Dennis, J., & William J. (2008). National Federal of Independent Business National Small Business Poll: Credit Cards. Retrieved July 23, 2012, from http://www.411sbfacts.com/files/SBP_V8I3_CreditCards_4%20(3).pdf

Documents Library (n.d.) Retrieved December 13, 2012 from https://www.pcisecuritystandards.org/security_standards/documents.php

Fewer Thefts of Credit Card Data May Reflect Effective PCS-DSS Standards (2012). Retrieved December 4, 2012 from http://www.siliconrepublic.com/strategy/item/30065-fewer-thefts-of-credit-card

Federal Trade Commission Act, Section 5, (15 U.S.C. §45).

Frye, C. (2006). PCI Council Focuses on Security Standards and Requirements. *Computer Weekly*. Retrieved December 9, 2012 from www.computerweekly.com/news/2240065965/PCI-council-focuses-on-security-standards-and-requirements

Gartner (2005). Gartner Survey of 1300 CIOs Shows IT Budgets to Increase by 2.5 Percent in 2005 [Press Release]. Retrieved January 21, 2013from www.gartner.com/press_releases/asset_117739_11.html

Gartner. (2006). Gartner Survey of 1400 CIOs Shows Transformation of IT Organisation is Accelerating [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=492238.

Gartner. (2007). Gartner EXP Survey of then 1400 CIOs Shows CIOs Must Create Leverage to Remain Relevant to the Business [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=501189.

Gartner. (2008). Gartner EXP Worldwide Survey of 1,500 CIOs Shows 85 Percent of CIOs Expect "Significant Change" Over Next Three Years [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=587309.

Gartner. (2009). Gartner EXP Worldwide Survey of More than 1,500 CIOs Shows IT Spending to Be Flat in 2009 [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=855612.\

Gartner. (2010). Gartner EXP Worldwide Survey of Nearly 1,600 CIOs Shows IT Budgets in 2010 to be at 2005 Levels. Gartner Press Release. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=1283413.

Gartner. (2011). Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011 [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=1526414.

Gartner. (2012). Gartner Executive Programs Worldwide Survey of More Than 2,300 CIOs Shows Flat IT Budgets in 2012, but IT Organizations Must Deliver on Multiple Priorities [Press Release]. Retrieved January 21, 2013 from www.gartner.com/it/page.jsp?id=1897514.

Gartner. (2013). Gartner Executive Programs Survey of More Than 2,000 CIOs Shows Digital Technologies Are Top Priorities in 2013 [Press Release]. Retrieved January 19, 2013 from http://www.gartner.com/newsroom/id/2304615.

Global Security Summit: Summary Report (2009). Retrieved November 18, 2012 from http://corporate.visa.com/_media/visa-security-summit-summary.pdf

Gorgone, J. T., Davis, G. B., Valacich, J. S., Topi, H., Feinstein, D. L., & Longenecker, Jr., H. E. (2002). "IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems," ACM, New York, NY and AITP (formerly DPMA), Park Ridge, IL.

MacCarthy, M. (2011). Information Security Policy in the U.S. Retail Payments Industry. *Stanford Technology Law Review*, 3-35.

MacCarthy, M. (2012). Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry. *I/S: A Journal of Law and Policy for the Information Society*, 245-279.

Messmer,E. (2012). PCI Council Publishes Risk-assessment Rules for Card-processing. Retrieved December 28, 2012 from http://www.networkworld.com/news/2012/111612-pci-264363.html

Minn. Stat. Ann §365E.64(2) (2007)

Morse, E. & Raval, V. (2012). Private Ordering in Light of the Law; Achieving Consumer Protection Through Payment Card Security Measures. *DePaul Business and Commercial Law Journal. 10*, 213-265.

Nev. Rev. Stat. §603A.215 (2010)

Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, version 2.0 (2010). Retrieved December 1, 2012 from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI DSS Self-Assessment Questionnaire (SAQ) (n.d.). Retrieved January 5, 2013 from https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Pepitone, J. (2012). 1.5 Million Card Numbers at Risk from Hack. Retrieved January 30, 2013 from http://money.cnn.com/2012/04/02/technology/global-payments-breach/index.htm

Rees, J. (2011). Tackling the PCI DSS Challenges, Retrieved October 7, 2012 from http://0-dx.doi.org.wncln.wncln.org/10.1016/j.bbr.2011.03.031

Segal, L., Ngugi, B., & Mana, J. (2011). Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem. *Fordham Journal of Corporate and Financial Law, 26*, 743-781.

Small Merchants Make up Lion's Share of Credit Card Breaches (2011). Retrieved February 7, 2013 from http://www.infosecurity-magazine.com/view/18022/small-merchants-make-up-lions-share-of-credit-card-breaches

Thapar, A. (n.d.) 10 Tips for a Successful PCI DSS compliance Project. Retrieved January 13, 2013 from http://www.verizonenterprise.com/resources/whitepapers/wp_pci-dss-compliance_en_xg.pdf

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, Jr., J. F., Sipior, J. C., & de Vreede, G. J.

(2010). IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. *Communications of the Association for Information Systems, 26,* 359-428.

Verizon 2011 PCI Compliance Report (2011). Retrieved December 10, 2012, from http://www.verizonenterprise.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf?__ct_return=1

Willey, L., Ford, J. C., White, B. J., & Clapper, D. L. (2011). Trade secret law and information systems: Can your students keep a secret? *Journal of Information Systems Education*, 22(3), 271-278.

Willey, L., White, B.J., & Stillwell, R. (2013). Student Perceptions of Business Compliance with Payment Card Industry Security Requirements: A Constructivist Approach. *Issues in Information Systems,* 14(1), 278-285

AUTHOR BIOGRAPHIES

Lorrie Willey, Assistant Professor of Business Law at Western Carolina University, earned a JD from the University of Tennessee and an EdS from Appalachian State University. Her interests include the application of law and ethics to business practices. Her articles have appeared in Business Law Review, Journal of Legal, Ethical and Regulatory Issues, Entrepreneurial Executive, Journal of Legal Studies Education and Issues in Information Systems.

Barbara Jo White, Associate Professor of Computer Information Systems at Western Carolina University, has a PhD in Business Administration from the University of Mississippi. Her interests include engagement work with IS students and local not-for-profit organizations. A Returned Peace Corps Volunteer, she has published manuals with Peace Corps and had articles appear in Decision Sciences Journal of Innovative Education, Issues in Information Systems, Small Group Research, Computers & Operations Research, Mountain Rise, Leadership and Organizational Development Journal and Business Communication Quarterly.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096