Implications of Visa's Cardholder Information Security Program upon Payment Processors

G. Orrie Gartner, Amir Madjdpour, Brian McMurray, Shailaja Subramanian

Orrie.Gartner@Colorado.EDU Amir.Madjdpour@Colorado.EDU
Brian.McMurray@Colorado.EDU
Shailaja.Subramanian@Colorado.EDU

A capstone paper submitted as partial fulfillment of the requirements for the degree of Masters in Interdisciplinary Telecommunications at the University of Colorado, Boulder, December 11, 2003. Project directed by Professor Douglas Sicker.

Abstract

Our thesis research intends to examine the technical and financial implications of CISP compliance on payment processors. Technically, the feasibility and implementation implications of this set of security standards relative to other standards currently in place were examined. Financially, a case study analysis on seven payment processors was performed in which the cost relative to company size was obtained. Compliance costs were then estimated for currently non-compliant organizations. The goal of this research is to show the potential impact of the CISP standards on payment processors, and will be useful to these organizations as well as the professional services organizations that assist them in this policy's implementation.

Introduction

The credit card industry has rapidly expanded over the past five years, and this trend is expected to continue. The Nilson report, a credit card industry information source, expects total credit card and debit transaction quantities to increase to over 60 Billion by 2007. The purchase volume of these transactions is expected to exceed $3 trillion by the same year [21].

Incidents of credit card fraud have increased along with the growth of the industry itself. A Gartner survey revealed that one in twenty consumers have been the victim of credit card fraud in the past year [20]. Similar studies estimate that the costs associated with these crimes approach $50 billion per year [19]. Identity theft, a popular form of credit card fraud, is the fastest growing crime in America, with 700,000 victims in 2002, and further research estimates that "Americans spent almost 300 million hours resolving problems related to ID Theft…." [19,2]. A study by the Gartner Group suggests these trends will continue, expecting "mass victimization" of consumers over a period of the next two years, and suggests that "consumers be extra careful to monitor all their financial transactions for unexplained account activity, withdrawals, or fund transfers [20]."

Institutions that digitally store and process credit card information must develop and institute policy that better ensures the privacy, security, confidentiality, integrity, and availability of this data.

What is Visa's Cardholder Information Security Program (CISP)?

In response to the growing security concerns regarding the credit card transaction process and industry itself, Visa U.S.A. announced its Cardholder Information Security Program (CISP) in April of 2000. By instituting CISP, Visa appears to be taking an aggressive stance toward securing cardholder information. While other major credit card corporations have suggested that 'best practice' security measures should be implemented in the networks of organizations that participate in the credit transaction process, Visa remains the only company mandating specific security practices. The CISP standard, designed to protect cardholders, merchants, service providers, and Visa from fraud and network attacks, is a compulsory compliance program applied to all organizations involved within the Visa transaction process.

CISP defines security standards designed to protect sensitive cardholder information. A set of twelve security guidelines, known as the "digital dozen", addresses various areas of security considered to be standard practice among the security community [4]. These CISP standards are to be implemented within the data networks of all businesses or organizations that store, process, or have access to Visa cardholder information including such as businesses as merchants, service providers, merchant banks, and others. To ensure an entity has properly and completely implemented all of these standards, an assessment and verification process must be completed by a qualified assessor.

Objective

This paper examines the Visa Cardholder Information Security Program and answers specific questions concerning the implications of the CISP standard on payment processors within Visa's transaction network.

Although CISP addresses all parts of the credit card transaction, clearing, and settlement process, the scope of this capstone will focus solely on a subset of Visa service providers known as payment processors. This group of companies process credit card transactions through the bank system; they are the intermediary between the merchant and the merchant's bank as they store, handle, and process cardholder data for Visa members.

Security consulting professionals with experience in CISP implementation as well as cooperation with Visa qualified assessors raised issues regarding the technical and financial implications for those complying with this policy. The research questions developed in tandem with these consultants are as follows:

1. **Do the Visa CISP Security and Audit Procedures for compliance go too far in mandating the implementation?**

2. **Do the costs associated with the implementation of Visa's Cardholder Information Security Program represent a burden to payment processors?**

Background

In order to understand the payment processor's role in the Visa network, a basic knowledge of the transaction process is required. Please see figure 1.

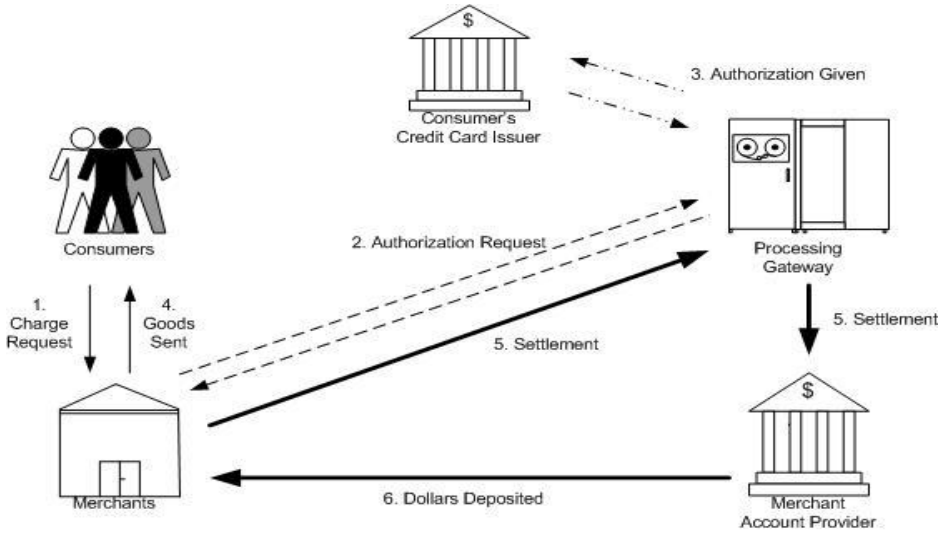

Figure 1: Transaction Process

When a consumer makes a charge request (step 1), the card is swiped and the credit card information and the authorization request is sent to a payment processor (step 2). The payment processor will then contact the customer's credit card issuer to determine that the account is valid and that the funds necessary to complete the transaction are available (step 3). If the credit card account and necessary funds are validated, the order is approved, and the merchant will fulfill the order (step 4). This is the end of the authorization cycle. The clearing and settlement cycle starts when the merchant sends a settlement request to the payment processor, which is often completed in mass batches in order to maintain lower per-settlement costs (step 5). The payment processor then contacts the consumer's issuing bank and requests that the proper funds be moved to the merchant's bank, which then routes these funds into the merchant's account (step 6).

Current Compliance

The preceding section demonstrates the integral role payment processors play within the Visa credit card transaction process and the reasons for security within this sector are clear. However, there has been considerable delay in most payment processors achieving CISP compliance. As of June 5, 2001, Visa stated that any entity subject to the CISP standard would be subjected to severe penalties including fines and operations restrictions if compliance was not achieved. As of September 11th, 2003, however, Visa had not yet set a date by which applicable organizations must validate their compliance and as a result only a handful of these companies have done so [22]. The CISP standards are viewed as fundamentally accepted security practices, yet the majority of organizations subject to CISP compliance still have not implemented these standards [4]. According to Jennifer Wallace-Fischer, a representative of the Visa CISP program, "the majority of CISP requirements are basic security requirements that all companies should already

have in place [5]." Research by ATC Security concerning CISP security implementation, however, demonstrates that most organizations do not currently have the necessary security required for CISP compliance. The following table shows the security implemented within the networks of the nine sampled service providers [18].

Table 1: Sampled firms and their current CISP compliance

	Firm 1	Firm 2	Firm 3	Firm 4	Firm 5	Firm 6	Firm 7	Firm 8	Firm 9	Totals
Firewall Installed	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	67%
Segmented Arch./DMZ	No	No	No	Yes	No	No	No	No	Yes	22%
Encrypted Data	No	Yes	No	Yes	Yes	No	No	No	No	33%
IDS	No	No	No	Yes	No	No	No	No	No	11%
File Integrity Monitoring	No	No	No	No	No	No	No	No	No	0%
Security Policy	No	No	Yes	Yes	No	No	No	Yes	No	33%
System Configurations	No	No	No	Yes	No	No	No	No	No	11%

Clearly the majority of firms have not put into practice the basic security mechanisms mentioned by CISP.

Previous Work

Most companies subject to CISP have delayed efforts to enhance the security within their networks until Visa imposes a firm compliance deadline. As of mid-November 2003, only seventeen payment processors had successfully completed the CISP review [6]. Because CISP is a relatively novel policy and so few organizations have implemented this standard within their networks and systems, little research exists regarding the implications of this policy on payment processors within the Visa transaction network. It is clear that this research and the questions posed above are now not only very timely, but quite important to those who work within the credit card industry, and those organizations that must implement these security measures.

Technical Analysis of Visa's CISP Security Audit Procedures and Reporting

The Visa CISP requirements have their roots in International Security Organization's (ISO) 17799, a security standard consisting of ten sections that describe best practices in information security, as well as the British Information Security Management Standard BS7799. The Visa CISP Security Audit Procedures and Reporting document was developed by Visa to be used as a guide in securing the enterprise and pertains to e-tailors as well as brick and mortar institutions. Visa maintains that these guidelines comprise a baseline standard that would be supported by the members of the security community [8,9]. Payment processors, as a subset of service providers, are required to follow these twelve guiding principles referred to as the digital dozen [7]:

1. Install and maintain a working firewall to protect data
2. Keep security patches up-to-date
3. Protect stored data
4. Encrypt data sent across public networks

5. Use and regularly update anti-virus software
6. Restrict access by "need to know"
7. Assign unique ID to each person with computer access
8. Don't use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly test security systems and processes
11. Implement and maintain an information security policy
12. Restrict physical access to data

While these principles by themselves look like common sense security measures, each requirement mandates additional detailed implementation measures. For example, specific time frames for examining logs are outlined, as are explicit encryption techniques such as SSL, PPTP, and IPSEC. Section 1.3 requires a corporation to "implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet." This specification additionally requires the use of "technologies such as Port Address Translation or Network Address Translation" to this end [10]. Such specificity could be cause for concern. If a security policy dictates overly detailed and universal network specifications including particular security tools and software products, it could result in somewhat identical network configurations throughout all organizations in compliance with that policy. Such cookie-cutter networks could increase the risk of attack throughout these organizations. For example, if Microsoft's IIS was the mandated web server, a weakness in this software discovered in one payment processor's network could likely be exploited in the networks of all other payment processors, inviting the possibility of large-scale attacks on multiple organizations. In addition, policy must be crafted that allows for flexibility in its implementation to account for the myriad network topologies in place throughout the networks of all payment processor. Furthermore, if a security policy is written with too much detail, advances in technology will make the policy obsolete. The following sections provide an analysis of the CISP requirements in order to determine if Visa went too far in mandating its implementation.

Comparing CISP

In order to determine the degree to which Visa mandates implementation of specific security measures, a comparison to a standard designed to protect electronic data was performed. Many computing standards exist that individually could provide a basis of technical comparison for specific portions of CISP. The Federal Information Processing Standards (FIPS) addresses a large range of security measures such as password issues and encryptions standards. The American National Standards Institute (ANSI), the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and other organizations all have various security standards in place. Though each of these organizations contains security policy segments relevant to CISP, none of them constitute a complete policy or best practice designed to protect the specific data addressed by the CISP standard.

It was determined that the Health Insurance Portability and Accountability Act (HIPAA) Security Matrix provided the most complete policy with which to base a comparison to CISP. Though the HIPAA standard is significantly wider in scope than Visa's CISP, Title II of this piece of legislation addresses the similar goal of ensuring the privacy and security of electronic data. In addition, the HIPAA Security Matrix is technology neutral, exhibiting implementation

flexibility [12]. Technological neutrality within the CISP standard would demonstrate similar flexibility regarding the implementation of this policy's technical standards. The HIPAA security matrix is a complete policy designed to protect patient data in the same manner CISP intends to protect Visa cardholder information. By systematically comparing these two technical documents, this section of the paper will determine if CISP does go too far in mandating implementation.

In addition to the technical document comparison, interviews were conducted with several payment processor regarding technical issues with CISP implementation. Two of the organizations interviewed provided information which will be included in this analysis.

CISP and HIPAA compared

The HIPAA security matrix consists of four sections: administrative procedures, physical safeguards, technical services, and electronic signatures. Within each section are specific requirements along with an associated implementation technique to be used, resulting in a layered, defense-in-depth approach to computer security. The requirements for each section (except for electronic signature which is not addressed by CISP) are illustrated in table two. This matrix compares the HIPAA requirements to those outlined in CISP's Security Audit Procedures and Reporting guidelines. Though the entire matrix could not be included in this paper due to space limitations, the portions that best illustrate the comparison follow.

Table 2: Communications/Network controls requirement within the Technical Security Services Section of HIPAA's Security Matrix and CISP's Associated Standards

HIPPA Implementation	Access Controls	Alarm	Audit trail	Encryption	Entity authentication	Event reporting	Integrity controls	Message authentication
CISP Implementation (section)	Restrict access to data by business need-to-know - role based (6)	Alert to unexpected compromise alerts (10.5)	Monitor system access attempts (7.3.10)	Encrypt transmission of cardholder and sensitive information across public networks (4)	Unique IDs, passwords, biometrics, tokens (7)	IDS and file integrity events (10)	File and data integrity (10.6)	Cryptographic solution (3.8)
	Access controls at user level (7)	Respond immediately to a system failure (10.7)	Enable audit subsystem (8.2.6)	Render unreadable stored cardholder data (3.7)		Firewall events (1.6)	System integrity (10.6.2)	
	Access controls to encryption keys (3.9.1)	Identify new vulnerabilities (8.3)	Track all user access to data (9)			Events on access to data (9)		
						User events (7)		

As table 2 illustrates, each implementation standard addressed by HIPAA's communications and network control requirement is also addressed by CISP. This is only one

specific requirement within HIPAA's technical section but it has been shown that for each of the requirements HIPAA makes, CISP addresses each in their Security Audit Procedures and Reporting document. Furthermore, CISP has similar obligations for each requirement in all three HIPAA sections. Clearly CISP is a well structured security policy, as it at least meets the requirements set forth by the United States federal government in HIPAA. However, this does not necessarily show CISP permits enough flexibility in its implementation.

Each security requirement from the twelve guiding principles was examined and checked for validity as well as the degree to which specific implementation measures and tools were mandated. For example, requirement 4.4 instructs users to encrypt all non-console administrative access to systems using technologies such as Secure Shell or Virtual Private Networks. Sending data in clear-text across the network is unacceptable within a secure environment and therefore this requirement provides a satisfactory level of security. In addition, the requirement does not go into too much detail by mentioning specific encryption methods, suggesting such options as SSH and VPNs but not ruling out others such as PCAnywhere. A payment processor may therefore use an application to administer a system remotely, as long as the transmission path is encrypted to the standards mentioned in requirement 4.3 (cryptography standards including at least 128 bit encryption). Requirements 7.3.1 through 7.3.13 address user passwords and include items such as requiring password changes at least every 90 days and ensuring a minimum password length of at least seven characters. All the requirements are clearly valid from a security standpoint. However, the policy does mandate seemingly minute details concerning the 15 minute timer on password protected screen-locks on workstations, which may seem as if the policy is dictating policy too specifically. However, though these standards may be on the stricter side, they are not at all unreasonable. For instance, although passwords must change every 90 days, standard security policies such as the SANS password policy suggests it should be every four months [15]. Ninety days does not seem unreasonable in an environment where protecting credit card data is of utmost importance.

One of the more difficult requirements to implement is section 3, protecting stored data [5,16,17]. This section requires cardholder data to be stored in an encrypted manner using any of a variety of approaches such as one-way ciphers, index tokens and pads, or strong cryptography, akin to 3DES or PGP, with the associated key management processes. Clearly it is not unreasonable to request sensitive cardholder data be stored in an encrypted manner and further review shows CISP does not go too far in mandating its implementation. For instance, it is not specified whether the encryption should be implemented in hardware or software, nor is one specific solution recommended over another. Though this section of CISP requirements may be more difficult to implement than other sections, the requirements for encrypting data do not dictate an unreasonable level of specificity.

Industry Implementations of CISP

For obvious security concerns, most organizations interviewed were reluctant to discuss specifics regarding their network infrastructure or actual implementation details of CISP. However, a CEO for one payment processor and a CTO for a second CISP compliant firm did provide some useful information. Both were asked if they were locked into a specific technical solution based upon the CISP requirements and whether they felt enough flexibility in the technical solutions for compliance existed. Each expressed that at no time did they feel tied to a specific solution.

This was reaffirmed in the distinct implementation approaches utilized by these two firms. One organization implemented the CISP security requirements within a Microsoft Windows environment while the other was based primarily on open source software. These differences reinforce the comparison results from above in which it was determined that the CISP requirements, although specific, do not mandate particular solutions [15,16].

Technical Analysis Conclusion

CISP does address all major aspects of computer security and mandates specificity in quite a few areas. However, this policy contains enough flexibility for companies to meet all the requirements given their current operating environment.

Economic Analysis

Visa mandates that all payment processors carrying or storing Visa cardholder information comply with the CISP standard, and in turn, assume the costs associated with the compliance and assessment process. As previously noted, a review of several payment processors which are not yet CISP compliant revealed that these organizations had only a small portion of the required security systems in place that would pass a CISP compliance audit. In order to achieve compliance, the remaining systems within these organizations would need to be upgraded and assessed at non-trivial expense. The costs associated with CISP compliance will be analyzed in this section, and it will be determined whether these costs represent a burden that could be detrimental to maintaining business operations.

Method

Of the 17 payment processors that are currently CISP compliant, phone interviews were conducted with representatives of the seven organizations within this group that agreed to provide data regarding CISP compliance costs. These representatives were asked to estimate the costs incurred by their organizations directly associated with becoming CISP compliant. Due to the nature of their business and unwillingness to disclose exact dollar figures for compliance costs, these data sets represent a rough estimation of the total CISP compliance cost. The cost estimates obtained were then graphed by company size according to total number of employees, and the resulting function was utilized to estimate the cost of CISP compliance for six public payment processors who are not currently CISP compliant. These public payment processors were selected due to the availability of their financial records, specifically operating costs, which was used in determining the relative impact of CISP-related costs. The public non-compliant companies ranged in employee number from 48 to 6000, which is fairly analogous to the employee range of the sample of compliant payment processors. The last step in our economic analysis was a comparison of the CISP cost estimates for these public payment processors to their total operating costs for 2002. This case study analysis concludes with general financial implications of this policy on payment processors regarding their ability to incur these costs and maintain normal business operations.

Calculating the Cost of Compliance

The cost of CISP compliance has two main components. The first component is the cost of purchasing and implementing the security measures. The cost associated with assessment by a Visa qualified assessor comprises the second component.

For most payment processors, network security tools such as firewalls, intrusion detection, and encryption systems need to be purchased and installed within their networks to ensure the level of security required by Visa. The implementation of this hardware, software and other equipment is also included within this cost component. Such costs may include installing and testing the necessary systems, hiring additional employees to perform the work and/or professional services expenses. For at least one payment processors, the resources required for such implementation is not trivial. This organization of fewer than twenty employees estimated that audit preparation consumed approximately 800 man-hours, representing a significant amount of resources relative to the size of the organization [16]. The expense associated with implementation of equipment depends on the amount of CISP compliant security hardware and software these organizations have prior to initiating the compliance process. Research of non-compliant service providers by ATC security, a qualified Visa assessor, revealed that CISP compliant systems such as a properly installed IDS and DMZ were in place in only 22% and 11%, respectively, of the organizations assessed. A security policy was in place in only one-third of these organizations. Chris Mark, Director of consulting services at ATC Security states that "Nearly all companies require some changes/upgrades to meet compliance with the CISP" [18]. An interview with the CTO of one firm suggested that this initial compliance figure for payment processors may be even lower. He learned through conversations with CISP assessors that most payment processors tend to have no more than 10% of compliant systems in place before the compliance process begins [15]. Such evidence suggests that most payment processors must purchase a considerable amount of security equipment and assume the cost associated with its implementation.

The second cost component is the on-site assessment cost. The CISP assessment is performed by assessors which complete the Visa certification process, and include such firms as Cable and Wireless and Ubizen, as well as various smaller auditors. Once organizations achieve initial compliance, Visa requires subsequent annual assessments to ensure that compliance to this standard is maintained. The costs associated with these subsequent assessments are not included in this analysis due to limited availability of data concerning this cost. The cost of assessment is dependent upon many variables, such as the particular assessor contracted to perform the work, the network topology and the assessor's level of familiarity with the organization. Experience to date suggests the cost range for CISP assessment is between $10,000 and $60,000. It is worth mentioning that the results of these assessments are not punitive. If the assessment and ensuing report reveals non-compliance issues, Visa requires that the payment processor develop a plan and firm timeframe to remedy these outstanding issues. In order to avoid penalties, the payment processors must implement all of the required deliverables according to the established timeframe [13].

Quantitative Analysis

Data collection

Table 3 displays the data obtained from the interviews conducted with the seven private payment processors.

Table 3: Estimated CISP Compliance Cost

Company Name	Number of Employees	Estimated CISP Compliance Cost
A	12	$150,000
B	40	$175,000
C	200	$400,000
D	2300	$500,000
E	5800	$600,000
F	11	$164,000
G	24	$250,000

Graphical Analysis

Figure 2 below indicates the relationship between the total cost of compliance and the number of employees based on the information provided in table 3. Though it was assumed that the 2002 transaction total for the payment processors interviewed would provide a more accurate representation of market-share, and therefore business size, than employee number, this data could not be obtained from several of these organizations. After plotting the seven available data sets, simple regression analysis was used to determine the curve that best fits the graphed points. The result is a logarithmic curve with the R^2 value of 0.95 and the related equation which represents the cost of compliance as the dependant variable. Again, it should be noted that this analysis lacks the sample size and exactness of data required to establish a tool that can accurately predict compliance costs for payment processors which have yet to begin the compliance process, and should be utilized only as an estimation of this cost. The graph below illustrates that as the number of employees increases, the total compliance cost increases.

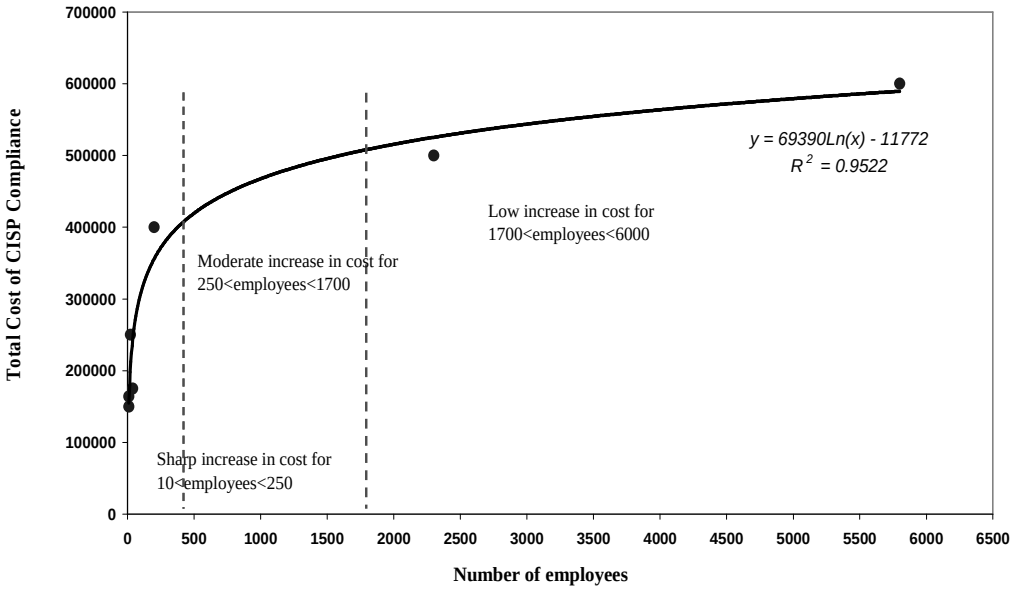

Figure 2: Compliance for Payment Processors

However, this increase is not linear. For a company with 10 to 250 employees, there is a sharp increase in cost of compliance. As the number of employees increases from 250 to 1700, the figure shows that the rate of cost increase begins to slow, and the cost increase becomes relatively stagnant for companies with more than 1700 employees. This suggests that companies with more employees, and presumably larger and more involved network topologies, may retain an advantaged position compared to the smaller payment processors regarding the relative cost of CISP compliance.

Estimation of the Cost for Non-Compliant Public Companies

Utilizing the formula shown on figure 2, the initial cost of compliance is estimated for six major public payment processors who are not currently CISP compliant. Table 4 represents the results of this cost estimation, using the number of employees for these companies as the input value for the mentioned formula.

Table 4: Cost of CISP compliance for public non- compliant payment processors

Company Name	Number of Employees	Gross Profit (Millions)	Operating Expenses (Millions)	Net income (Millions)	Esimtated Cost of CISP Compliance	Percentage of Operating Cost
Global Payments	1,700	$255.794	$162.529	$53.300	$504,377	0.31
Total System Services	5,121	$423.723	$266.050	$31.736	$580,895	0.22
Electronic Clearing House Inc.	162	$7.532	$11.201	-$2.376	$341,256	3.05
National Processing Inc.	1,800	$124.858	$43.334	$51.077	$508,344	1.17
eFunds Corp	4,500	$131.237	$95.818	$24.554	$571,925	0.60
Payment Data Systems	48	-$0.483	$7.798	-$10.995	$256,851	3.29
Bottomline Technologies	389	$35.356	$49.197	-$27,854	$402,041	0.82

The last column on the table shows the percentage of year 2002 operating cost comprised of costs related to CISP.

Economic Analysis Conclusion

This case study suggests that, in general, smaller companies are impacted to a greater extent relative to larger companies by CISP compliance costs. In our analysis, the payment processors most significantly affected by the costs related to CISP were Payment Data Systems, Electronic Clearing House, Inc. (ECHO) and Bottomline Technologies. For all three of these organizations, the costs associated with CISP weaken their already vulnerable financial position. For Payment Data Systems and ECHO, their competitive position may be further weakened due to the fact that CISP costs represent a larger percentage of operating costs relative to their competitors at 3.29% and 3.05%, respectively. The cost related to achieving CISP compliance, though fairly insignificant to larger payment processors, have the potential to further weaken the position of financially susceptible firms within this sector. Under the Risk Factors section of ECHO's 2002 10-K report, the company states "As the compliance issues become more defined in each industry, the cost associated thereto may present a risk to *ECHO*. These costs could be in the form of additional hardware, software or technical expertise that *ECHO* must acquire and/or maintain. While *ECHO* currently has these costs under control, it has no control over those entities that set the compliance requirements so no assurance can be given that *ECHO* will always be able to underwrite the costs of compliance in each industry wherein it competes [23]."

Conclusion

The analysis regarding the technical requirements mandated by CISP included a comparison of the CISP standards to the HIPAA security matrix, an analysis of each CISP condition against standard security practices, as well as first hand interviews. This analysis showed that this policy provides firms the necessary flexibility to meet all of its requirements and that the policy does not go too far in mandating its implementation. Regarding the financial implications of this policy, the case study analysis suggests that the costs associated with CISP compliance should not threaten the ability of financially stable payment processors to sustain normal business operations. However, these costs potentially represent a threat to payment processors incurring significant losses and maintaining limited cash resources. Further research in this area could include such topics as the potential for this policy to spur consolidation within this sector and the application of the CISP security platform for other credit card companies or industries.

References

[1] "Still Secure: Reducing Your Risk Has Never Been This Easy."
http://www.stillsecure.com/docs/VISA_CISPandStillSecure_BG.pdf, October 28, 2003.
[2] Whelan, Christine B. "How to Strike Back at Identity Theft." *Wall Street Journal* 21 Aug 2002: D1
[3] Dignan, Larry. "DPI Scrambles After Credit-Card Theft,"
http://www.baselinemag.com/article2/0,3959,920281,00.asp, March 6, 2003.
[4] Desmond, Paul. "Visa is monitoring merchants for security compliance,"
http://www.esecurityplanet.com/trends/article.php/688812, June 1, 2001.
[5] Wallace-Fischer, Jen. Email Interview, October 8, 2003.

[6] "List of Compliant Service Providers as of 10/10/2003," http://usa.visa.com/media/business/cisp/List_of_CISP_Compliant_Service_Providers.pdf , October 28, 2003.
[7] "Cardholder Information Security Program," http://www.visa.com/cisp, October 27 2003.
[8] Levitt, Jason. "Security – The Enemy Within," http://www.informationweek.com/834/secure.htm, October 12l 1, 2003.
[9] Imhoff-Dousharm, Robert. "Credit Card Networks 101. What they are, and how to secure them," presented at DefCon 11, Las Vegas, Nevada/USA, August 1, 2003. notes available at http://www.j3sus.net/defcon/images/defcon-11/dc-11-presentations/dc-11-Imhoff/Credit-Card-Networks-101.pdf
[10] "Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting as of 8/8/2003," http://usa.visa.com/media/business/cisp/Security_Audit_Procedures_and_Reporting.pdf, October 27, 2003.
[11] "Shackled by the rules? Unlock the opportunities," http://www.scmagazine.com/scmagazine/2003_02/cover, November 2, 2004.
[12] "HIPAA – Addressing the Technical Requirements," http://www.watchguard.com/infocenter/whitepapers.asp , October 15, 2003.
[13] "Visa USA Cardholder Information Security Program: Merchant and Service Provider Q &A." http://usa.visa.com/media/business/cisp/Merchant_and_Service_Provider_QA.pdf, August 6, 2003.
[14] "SANS Security Policy Project," http://www.sans.org/resources/policies, November 9, 2003.
[15] "Personal Interview with CTO of major credit card processing company who wanted to remain anonymous," October 8, 2003.
[16] "Personal Interview with CEO of major credit card processing company who wanted to remain anonymous," October 14, 2003.
[17] "Personal Interview with VP of managed security service Company who wanted to remain anonymous," September 4, 2003.
[18] Mark, Chris. "Visa CISP Assessment Overview," *Electronic Transactions Association Conference*, October 23, 2003.
[19] "Federal Trade Commission Identity Theft Survey Report," http://www.ftc.gov/os/2003/09/synovatereport.pdf, September 2003.
[20] "Identity Theft Statistics," http://www.identity-theft-protection.com/stats.html, November 18, 2003.
[21] "The Nilson Report," Issue 797, October 2003. pg 4-5.
[22] Email Interview with Visa CISP Team. September 11, 2003.
[23] "Electronic Clearing House, Inc. Form 10-K," http://www.echo-inc.com/ECHO_Form%2010K_12_27_final.pdf, November 18, 2003.