Global Information Assurance Certification Paper

Visa's Digital Dozen:
The Cardholder Information Security Program (CISP)

Mark Franz

GIAC Security Essentials Certification (GSEC)
Version 1.4b
Option 1

Submitted July 5, 2004

Table of Contents

Abstract

Within the past few years we've seen a significant number of regulations introduced that impact the security community. Most security professionals would have no trouble listing off numerous government regulations such as HIPAA, Sarbanes-Oxley and California HB-1386.

Financial institutions are among many industry segments that encounter specific governmental oversight. Regular reviews monitor the uniform principles that are enforced by any number of agencies, such as the Federal Reserve Board, Office of Thrift Supervision and the Office of the Comptroller of Currency (among others).

In addition to the formal regulatory and legal environment we're beginning to see programs pop-up that are designed to allow and promote self-regulation. Among these is Visa's Cardholder Information Security Program (CISP).

Why did Visa create the CISP?
What is the CISP?
What does it mean to me?
How do I survive the audit and ensure compliance?

The rest of this paper will attempt to answer these questions and provide some guidance from someone who has seen it first-hand.

Introduction to the CISP

So just what is the CISP?

The Computer Security Dictionary has this to say about it:
"Visa's CISP defines a standard for protecting cardholder information. It is an ongoing development, where the initial effort has focused on the e-commerce acceptance channel, including an active program to ensure annual validation of selected, major e-merchants' security positions"[1]

In more simple terms if you store Visa Card information you are responsible for handling that information according to Visa's rules and regulations.

A part of a larger security commerce program (which includes Verified by Visa as well as Visa's "Operating Regulations") the CISP was approved in 1999, introduced in 2000, and mandated beginning in 2001. It appears to have been initially been targeted to reduce "online" credit card fraud. Reaching this interpretation doesn't require much interpretation. The Security Encryption News website[2] references an August 11 Computerworld article, reporting that:

- A Gartner Group Inc. survey indicates "credit card fraud is 12 times higher for online merchants than their offline counterparts", and
- "Brian Buckley, Visa's vice president for product risk and analysis, said these security initiatives are expected to reduce Internet transaction disputes by up to 50%".

Visa understood that E-commerce and online shopping were rapidly booming, and more importantly that the perception of security (or lack thereof) was a barrier to consumer confidence. In a case study presented in April 2002 to the High Performance Computing and Communication Council Pamela Mallet, Director of E-Commerce Risk at Visa USA, cited several sources indicating "Credit Card Security" as the number one concern expressed by consumers regarding e-commerce[3].

With this knowledge in hand Visa set out to lend a helping hand by creating a set of guiding principles that would remove the perception of security risk in the e-commerce world. The CISP is born.

---

[1] Itsecurity.com Dictionary+ of Information Security. URL: http://www.itsecurity.com/dictionary/cisp.htm (July 5, 2004)
[2] Security and Enryption News. URL: http://www.security-encryption-news.com/news09.htm (August 11, 2000)
[3] A Case Study: Visa USA's Cardholder Information Security Program, by Pamela Mallet, High Performance Computing Council Website. URL: http://www.hpcc-usa.org/pics/02-pres/mallett.ppt (April, 2002)

So we understand that e-commerce was the initial target. What now? As we review the CISP definitions provided above there are a couple of key phrases that stick out:

- "It is an ongoing development", and
- "Cardholder data, wherever it is stored".

From its inception the CISP was intended to start with a small scope, specific targets were defined in the e-commerce arena. Through it's short lifetime it has, by Visa's design, developed and expanded with an end goal of implementing the standards for all Visa cardholder data.

Ok, that was an interesting history lesson; but enough of that. Specifically what is the CISP?

The Digital Dozen

In simple terms the CISP outlines twelve requirements, commonly referenced as the "digital dozen" (or sometimes as the "dirty dozen"). Visa's CISP website provides ample reference to these requirements, including general information about the program, applicability information, questionnaires, FAQs and other review information. While we don't need to just echo information that is readily available at the site it is worth at least pulling the list of the digital dozen from it.

The CISP Requirements

Here, from Visa's website[4], is the appropriate definition of the CISP:

- An easy to remember list of 12 basic security requirements with which all Visa payment system constituents need to comply
- More detailed sub-requirements, always tying back to the CISP requirements

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.

[4] Visa's Cardholder Information Security Program website. URL: http://www.visa.com/cisp (Referenced July 5, 2004)

Hmmm, so you say that you don't see anything here that you haven't seen before with other programs and standards?

Absolutely right! For those companies and organizations that have methodically applied common standards and practices such as the SANS Security Essentials, ISO 17799, or the CISSP 10 Domains there will be nothing particularly alarming about the program.

Although the requirements are so readily reflected by other security programs why would Visa go to such trouble to create "yet another program"? Here's the rub. Despite a regulatory requirement that mandates protection of not only card data but of personal data not everyone is diligent in their efforts to apply even minimal security standards.

Armed with this understanding Visa set out to better define the due care required for Visa cardholder data. The CISP program is but a portion of an overall program Visa is defining in hopes of reducing fraud.

In an article posted on the International Card Manufacturers Association website John Shaughnessy of Visa USA outlines several programs that are now in place with the end-goal of preventing fraud and improving Visa customer confidence. Speaking specifically of the CISP he has this to say[5]:

> "While there is no such thing as a magic silver bullet when it comes to security, the CISP requirements are regarded as the payment-industry standard for online data security. In fact, CISP was the first such standard in the payments industry and served as the model for best practices published by the G-8 at their 2001 Conference on High-Tech Crime in Tokyo.The good news is that these safeguards are working."

Why Comply?

Ok, so the CISP program appears to be a step in the right direction. While it is called friendly "helping hand" it does result in something along the lines of a standard of due care for Cardholder data it also becomes yet another "audit program".

Why should we bother? After all, we do pay attention to security and don't have time for another audit?

Visa has frequently been quoted as indicating three primary reasons why an organization would *want* to comply.

[5] "Taking Action Against Identity Theft", International Card Manufacturer's Association website. URL: http://www.icma.com/info/takingaction91003.htm (referenced July 5, 2004)

- Create a competitive edge by allowing consumers to trust your environment over others.
- Improve your profit picture by reducing the likelihood of chargebacks and losses.
- Maintain your image.

In addition to referencing these benefits Mark Merkow appropriately summarizes the teeth that the program will carry in a posting to internet.com[6]:

> "Serving as both a carrot and a stick, the CISP helps Visa to accelerate their demands on merchants to do a much better job of credit card security than what's been seen in the past. The new Visa USA Operating Regulations include a monitoring and compliance program that will take effect this year. Failing to live up to these regulations places your ability to accept Visa cards on your Web in jeopardy. Besides that, implementing these countermeasures and compensating controls is simply the *right thing to do!*"

As we can see, enforcement of Visa's programs will carry substantial penalties. With the CISP, initial penalties might include simply fines and financial incentives. However, the penalties may not remain solely financial; as indicated you could lose your ability to accept Visa cards.

Aside from the enforcement, Mark's final statement is probably the best we can cite; it's the "right thing to do".

Understanding and Implementing the CISP

Through this point we've covered a bit of a history of the CISP, reviewed from a high level what the CISP requirements are and from a (hopefully) realistic perspective an understanding of just why this program is important enough to implement.

What next? Much of this answer comes from understanding the degree to which you've already implemented valid security practices. For those that have been diligent with one of the many standards or "best practice" models the work will be minimal. Organizations that haven't been as diligent, well, the security posture will likely improve significantly through the audit and compliance program.

There are continued references to "best practices". It's very true that most of the requirements and sub-requirements will fit nicely into the best practices models. Cited most frequently are the SANS Security Essentials and the CISSP Ten

[6] Visa Helps Safeguard Electronic Payment Card Data, Internet.com eCommerce website. URL: http://ecommerce.internet.com/how/tk/article/0,3371,10366_739361,00.html (April 10, 2001)

Domains. While these generally "fit", they are neither an exact match nor a complete list.

That's right, the CISP is not a complete list. If Visa is so concerned about the security of the cardholder data, and if the security industry's best and finest develop standards and best practices then how can this be explained?

What's Missing?

The answer is really not all that difficult when we look at the fundamental principles of security.

In Shon Harris' book the "All In One CISSP Certification Exam Guide"[7] he clearly describes the Fundamental Principles of Security by referencing the *AIC Triad*. Frequently referenced as the three pillars of security Availability, Integrity, Confidentiality are the fundamentals of security. The most indicative line in his description tells us that "The level of security required to accomplish these principles differs per company because their security goals and requirements may be different."

This is never more evident than when we look at the CISP. The Availability principles are nearly missing. Does this mean that Visa doesn't care about availability? Hardly, but the program's main focus is on the Confidentiality of the cardholder data (with injections of Integrity).

Is this a problem? It could be, but it doesn't need to be. The danger is that an organization that is successful in passing a CISP audit after focusing solely on the CISP requirements may fall short on the needs for availability.

What's Added

What if my organization is diligent with practicing security just as the SANS Security Essentials suggest? Are there things I need to know about that might fall outside of what we regularly look at?

Again, this answer is pretty basic. From a high level the CISP doesn't require anything that a sound security program doesn't already enforce. However, we need to remain aware that this is a program that is specifically focused on Visa Cardholder Data. With that in mind we there are a few things that are "over and above" what might normally constitute sound security.

The best example of this is that organizations are not to store CVV2 (card verification value) data or data stored on the magnetic stripe of the card. Period.

[7] Harris, Shon, "All in One CISSP Certification Exam Guide Second Edition", New York: McGraw Hill/Osborne, 2003, page 53.

Sound practices may tell you that if you have a system that "uses" these values that you can build appropriate direct or compensating safeguards and avoid a CISP compliance issue. But in chatting with various security folks (including auditors) it has become evident that Visa will be quick to tell you that this is a direct violation of not only the CISP but of the Visa "Operating Regulations". No amount of compensating controls will resolve the finding.

The Compliance Process – A few tips from experience

Until now we've been trying to outline enough information about what the CISP program is, its focus, and the need to pay particular attention to a few of the requirements. We also know that if not already, Visa will require our organizations to comply with the program. So what's the process?

We'll now delve into the compliance program, not so much from a formal program perspective but from my personal perspective; that of someone who has gone through the formal audit process already.

Everything needed for the formal program is included in Visa's CISP website (www.visa.com/cisp) so we won't be simply echoing what's readily available there. Besides the requirements are changing, so it will be necessary to revisit them frequently to make sure the changes don't catch you off-guard.

Visa does have a plan for moving the program forward, including an increasing net of organizations that it expects to receive formal compliance. Keep this in mind. If Visa hasn't already called you, expect a call at some point.

This doesn't mean you have to wait until they call. Remember, if you deal with Visa cardholder information you are expected to comply. As reviewed earlier there may be business advantages that come along with compliance.

Getting Started

One of the things that I found particularly useful in preparing for our organization's review is the Visa USA Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting checklist[8]. This is the actual audit checklist and reporting tool that will be used by the auditor you will be selecting.

If your audit hasn't started visit the website regularly to pick up the most recent version. It does occasionally change. Like any good audit program the

[8] Visa Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting as of 3/1/2004. URL: http://usa.visa.com/media/business/cisp/Security_Audit_Procedures_and_Reporting.pdf (March 1, 2004)

procedures and reporting information available at the start of your audit will govern the entire audit. It is a point-in-time review, not a rolling target.

Remember that this will be a recurring audit. Even if you have an active review and understand what the current requirements are you will be subjected to a new review next year. Keeping up with the requirements will help you better prepare.

With the auditing tool in hand, it should be relatively simple to conduct a self-audit. You should already have many or most of the answers, so a brief trip through the process won't be particularly time consuming. For those items that you don't have ready answers to, find them (your auditor will be asking anyway, why not prepare?).

Doing this early (hopefully long before Visa *requires* your formal audit) should allow ample time to make corrective actions. If your organization balks at the idea of spending the time or money at this point simply remind them that enforcement won't be far around the corner.

The Auditor

One of the things that occurred early in the program was the ability to select any services firm to do a CISP audit. Armed with the checklist any firm could handle the work. This lead to quite a disparity with the quality of the audits; from inexpensive one or two day reviews to very thorough reviews with three or more weeks of field work.

Thank goodness Visa recognized this flaw and has worked diligently at creating appropriate standards for the audit teams leading to an approved list of auditors. The approved vendor list is on the CISP site[9]. This list is currently frozen, so additions to it are not likely in the near future.

Given Visa's diligence in correcting this problem the disparity of results will no longer be of issue. However, having seen both the good and not-so-good sides of the early program (through our own audit and those of business partners) it became evident that finding the correct audit firm was of critical importance.

The firm we selected had conducted several CISP audits prior to ours and had developed a very good relationship with the CISP program personnel. Through this experience the audit team had a firm grasp of the true intent of the program and, by facilitating discussions between Visa and ourselves we were able to maintain compliance on several issues where we didn't meet the "letter of the law" but certainly met the "full intent" through compensating controls.

[9] Visa USA Cardholder Information Security Program (CISP) Qualified CISP Security Assessor List as of 6/28/2004. URL: http://usa.visa.com/media/business/cisp/Qualified_CISP_Assessor_List.pdf (June 28, 2004)

While I'm sure each of the firms currently listed on Visa's list would provide adequate coverage in this area I would highly recommend validating the track record of the candidates that you might consider. Ask for references. Make sure your audit team has developed a relationship with Visa.

Know the Scope

Visa's "digital dozen" is indeed a set of twelve "easy to remember" items that define a standard of diligence. But it's not quite that easy. Each of the requirements is broken into several sub-requirements; all of which must be honored. The devil's in the details, as they say. Visa is very quick to point out that each of the sub-requirements is intended to enforce the main requirement; yet it's easy to let a sub-requirement get out of hand.

As good example, from our own organization's CISP audit we have a number of network devices that "were" managed via a terminal server; this terminal server was sufficiently "legacy" that it was not SSH compliant. The audit team found this and this showed up on the initial report as non-compliant under requirement 4.4 "Encrypt non-console administrative access".

Despite this we were able to demonstrate compliance for this topic. How? We could have argued that the subnet on which the terminal servers were used was tightly controlled. Compensating controls work well in most cases.

But the answer was much more simple than that. The main requirement (Requirement 4) tells me something along the lines that I need to encrypt transmissions across *public networks* (e.g., the Internet). Since we did not allow administrative access over anything but our internal (private) network we were not non-compliant.

Now, don't mis-understand this. I would never argue against the merit of implementing SSH for ALL administrative and console access, a sound overall security program would require it. I only cite this as a simple example to illustrate that understanding the scope allowed me to retain a reasonably clean report and correct the issue on my own terms and in my own time.

Be Honest, and Be Realistic

This probably goes without saying, but with any audit honesty is a mandatory trait. Yes, non-compliance and corrective actions can be painful. But trying to hide things serves no common good; and frequently a thorough audit field staff will discover the dishonesty anyway.

As well, when it comes to working out the corrective actions, be as realistic as you can. If you need a major infrastructure change it's not going to happen overnight; and in all likelihood it will take a cross-organizational effort.

Make sure, when you submit a corrective action, that if another organization's effort is required that you get their buy-in and support. Proof of correction is required and Visa does follow up on non-completed business.

Interaction with Other Programs

There are other programs that are similar. Will compliance to one ensure compliance with the other?

There seems to be some discussion and not yet a significant agreement between the various card companies on this topic. According to Holli Hart Targan in a recent Transactionworld.com article: "Visa, MasterCard, Discover and American Express representatives stated at the ETA meeting in September that they would not oppose standardizing such requirements, and I understand they are working toward that end. It would be welcome relief."[10]

It seems that, at least for the short term, the answer is that each program will require compliance. We can only hope for a longer term agreement.

What this doesn't close is the option of combining multiple audits into a single review. Speaking of our current scenario we have closely investigated the possibility of combining our annual CISP review with one or more of our other audits, such as our "internal audit" (which is conducted by an outside firm).

Although we have not taken this step yet the audit firms appear receptive to the idea as long as this type of work doesn't cross the lines of segregation being enforces under other regulations such as Sarbanes-Oxley. Each organization must ultimately make it's own decision; however, this is something we will likely pursue with our next annual CISP review.

Summary

We've taken a brief history lesson on the CISP program and dug a bit deeper into why Visa might have created such an aggressive step by creating the program. And hopefully the brief insight and tips provided by the author in his travails with CISP compliance will be helpful to the readers.

What bears repeating from the paper is that if you and your organizations have been diligent in your application of *some* security standard or some security model that you'll generally not have trouble with CISP compliance.

[10] Transaction World Card Association Update, "Get Tough on Data Security". URL: http://www.transactionworld.com/articles/2004/February/cardAssocUpdate1.asp (February, 2004)

References

Itsecurity.com Dictionary+ of Information Security. URL: http://www.itsecurity.com/dictionary/cisp.htm (July 5, 2004)

Security and Enryption News. URL: http://www.security-encryption-news.com/news09.htm (August 11, 2000)

A Case Study: Visa USA's Cardholder Information Security Program, High Performance Computing Council Website. URL: http://www.hpcc-usa.org/pics/02-pres/mallett.ppt (April, 2002)

Visa's Cardholder Information Security Program website. URL: http://www.visa.com/cisp (Referenced July 5, 2004)

Taking Action Against Identity Theft, International Card Manufacturer's Association website. URL: http://www.icma.com/info/takingaction91003.htm (referenced July 5, 2004)

Visa Helps Safeguard Electronic Payment Card Data, Internet.com eCommerce website. URL: http://ecommerce.internet.com/how/tk/article/0,3371,10366_739361,00.html (April 10, 2001)

Harris, Shon, "All in One CISSP Certification Exam Guide Second Edition", New York: McGraw Hill/Osborne, 2003, page 53.

Visa Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting as of 3/1/2004. URL: http://usa.visa.com/media/business/cisp/Security_Audit_Procedures_and_Reporting.pdf (March 1, 2004)

Visa USA Cardholder Information Security Program (CISP) Qualified CISP Security Assessor List as of 6/28/2004. URL: http://usa.visa.com/media/business/cisp/Qualified_CISP_Assessor_List.pdf (June 28, 2004)

Get Tough on Data Security, Transaction World Card Association Update. URL: http://www.transactionworld.com/articles/2004/February/cardAssocUpdate1.asp (February, 2004)