



Leadership
Benefits
Results

Newsletter—1st Quarter

Join Today and receive a \$50 coupon in Member Enhancements!

apply online:

[CLICK HERE](#)

Call to Join
877-378-4378

To Submit an Article Idea, please

[CLICK HERE](#)

To Post Comments to this Article

[CLICK HERE](#)

NEWSLETTER ARCHIVES

Articles of interest for the Executive Suite Industry:

If You Accept Credit Cards, You'd Better Pay Attention!

Greg Johnson, PCI Consultant
Security Metrics

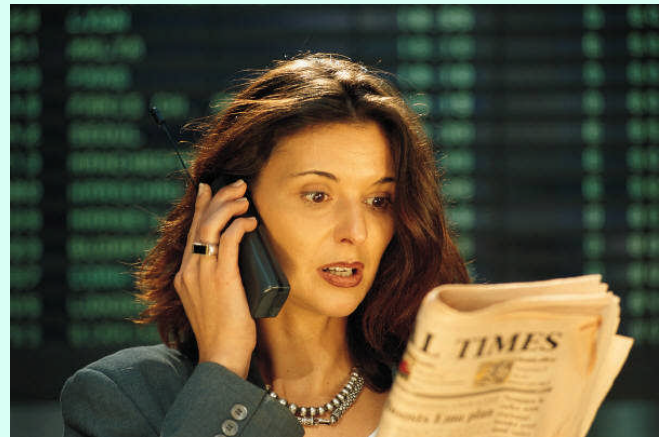
Security Metrics simplifies merchant compliance



The recent data compromise of large retailer T.J. Maxx captured our attention. Although Internet credit card compromise is not new – in recent years hackers have even broken into giants such as Amazon.com – such headlines cause us to wonder *just how safe is e-commerce?*

The Good News:

Visa has begun leaning on members, merchants and service providers to ensure compliance with its Cardholder Information Security Program or CISP, a program designed to protect Visa cardholder data everywhere.



Editor's Note:

Historically, good security services have been expensive. The cost of security consultants, personalized software, and perpetual maintenance has kept adequate Internet security out of reach of most Internet-connected businesses. Our dealings with Security Metrics have resulted in our soliciting an article from them for your benefit. They are both knowledgeable, and experienced as well as able to communicate in plain language — and their customer service is well above par. The idea of PCI compliance and the issues surrounding it are quite daunting, to say the least, and the fines and penalties are scary. We wanted to bring you insight from a group dealing with this daily to help inform, protect and prevent any negative consequences for your centers. ☞



Leadership
Benefits
Results

Newsletter—1st Quarter

Join Today and receive a \$50 coupon in Member Enhancements!

apply online:

[CLICK HERE](#)

Call to Join
877-378-4378

To Submit an Article Idea, please

[CLICK HERE](#)

To Post Comments to this Article

[CLICK HERE](#)

NEWSLETTER ARCHIVES

Further, in September of 2006, a joint body called PCI Security Standards Council, composed of a cooperative effort between Visa, American Express, Discover and MasterCard, became empowered to develop the Payment Card Industry (PCI) Data Security Standard (DSS.)

Why is this Good News?

When a merchant or service provider is PCI certified or compliant, it means that typical “back doors” to critical data have been locked to hackers. Though there are no guarantees, a PCI certified merchant or service provider is far less likely to be compromised. Hackers will look for easier open doors. The result – safety and confidence for consumers!

Recently, the card companies have been putting immense pressure on all of their members to become engaged with a qualified PCI assessor by March 31 of this year, and fully compliant by September 31. What this means for you if you’re a merchant is that failure to do so will result in potential fines and fees – fines that have been known to hit \$500,000 per incident if data is compromised and the merchant is not in “Safe Harbor” or in other words, is PCI certified!

Card companies will now only offer prime discounts to PCI compliant merchants and service providers, and the day is swiftly coming in which non-compliant merchants will not be able to accept credit cards. The *big* carrot is customer confidence in the security of precious credit card and personal information. This will translate to increased sales.



According to NWAnews.com, (for full article see <http://www.nwanews.com/adg/Business/167849/>) “MasterCard Inc. and Visa USA Inc. are clamping down on merchants that flout rules aimed at protecting card transactions from fraud. “

“MasterCard has imposed fines on merchants that haven’t met its requirements to keep transactions secure. Visa will take aim at the nation’s largest merchants with fines that start at \$ 10,000 a month and can rise to \$ 100,000 a month. “



Leadership
Benefits
Results

Newsletter—1st Quarter

Join Today and receive a \$50 coupon in Member Enhancements!

apply online:

[CLICK HERE](#)

Call to Join
877-378-4378

To Submit an Article Idea, please

[CLICK HERE](#)

To Post Comments to this Article

[CLICK HERE](#)

NEWSLETTER ARCHIVES

To better understand how this works, “Visa and MasterCard don’t fine the merchants directly. Instead, they levy fines against those that process the transactions on behalf of the merchants. Those entities commonly pass on the fines to their merchant customers. In addition to assessing penalties for failing to comply with the rules, Visa and MasterCard also issue separate fines if a noncompliant merchant has a security breach. “



So What Do I Need to Do?

Starting the compliance process is simple.

Contact an authorized assessor such as Security Metrics, pass their network scan and answer a Self-Assessment Questionnaire. *Unless you’re a Level 1 Merchant, meaning you do 6,000,000 transactions per year and need an annual audit, this applies to you.* There are several steps involved in compliance:

- The network scan looks at your web sites and network devices that have what’s called a publicly available IP address. IP (Internet Protocol) addresses are like phone numbers – they identify servers and equipment that exist on the Internet.

These IP addresses are how hackers enter your system and find critical data. The network scans will look for open doors (called ports), and vulnerabilities that render data susceptible to theft and attack.

- The PCI Self-Assessment Questionnaire contains 75 questions regarding network security and practices. If computers and systems are not your forte, not to worry – Security Metrics personnel will answer your questions, consult and advise until you can pass the assessment and scans. That’s it!

This mandatory investment in PCI certification will pay off in the long run. For example, recently an e-commerce vendor called Security Metrics to perform a forensic investigation. A forensic is an audit which VISA and MasterCard mandate when card data is compromised (hacked.)

Unfortunately, this particular merchant was not compliant, and the data on the compromised disk drives was not encrypted (PCI rules state that stored cardholder information *must* be encrypted.)



Leadership
Benefits
Results

Join Today and receive a \$50 coupon in Member Enhancements!

apply online:

[CLICK HERE](#)

Call to Join
 877-378-4378

To Submit an Article Idea, please

[CLICK HERE](#)

To Post Comments to this Article

[CLICK HERE](#)

NEWSLETTER ARCHIVES

Newsletter—1st Quarter

For this small e-commerce merchant, this event meant a very expensive forensic audit, a required annual audit, and forthcoming fines. Had the merchant been compliant, or under Safe Harbor, he would have saved almost *eighty times* the cost of the compliance process – not to mention lost customer confidence!

A Call to Action!

PCI compliance for small merchants is usually accomplished within thirty days at an average cost of \$199 per web site or IP address. The price of the service is a small one compared to the safety and security of data, and consumer confidence in the business.

Security Metrics also offers a free PCI Evaluation Scan. Follow this link, and once you complete the online form, a link will be emailed to you to start your FREE PCI Evaluation Scan.

https://www.securitymetrics.com/eval_scan.adp

About Security Metrics: A privately held company, Security Metrics is one of only three vendors in the US authorized for all major PCI security services. Founded in 2000 to secure networks from intrusion and compromise, the company is an authorized PCI provider for Visa, MasterCard, American Express, and a recognized provider for acquiring banks such as Bank of America, Transfirst, First Data, and RBSlynk. Security Metrics may be reached at 801-705-5661, or gregj@securitymetrics.com.

For more in depth information regarding the PCI Compliance, visit <https://www.pcisecuritystandards.org/index.htm>, the website for the PCI Security Standards Council. They provide complete details and oversight for this important development in credit card processing.