SecurityMetrics

Jake Young
Dir. Business Development

SecurityMetrics protects electronic commerce and payments leaders, global acquirers, and their retail customers from security breaches and data theft. The company is a leading provider and innovator in merchant data security and compliance, and has helped over 1 million organizations as an Approved Scanning Vendor and Qualified Security Assessor.

What do you see as an ISO's largest PCI 3.0 implementation challenge?

Merchants probably won't care for the big changes in PCI 3.0, such as new SAQs and extensive documentation requirements. It will be nearly impossible to avoid the, "I've never been a fan of PCI, and now you're telling me I have even more requirements?" merchant reaction.

The best way to avoid irritated merchant feedback is proactive communication through as many mediums as possible, ASAP. Upload a PCI 3.0 banner on your merchant website. Enlist the help of your PCI partner to send explanatory emails. Utilize social media to share PCI 3.0 information. Ask your PCI partner to hold and record a webinar explaining new PCI 3.0 requirements and demonstrate how to simplify the complex process. In all communications, include a customer service phone number and a support email that's reviewed regularly.

How can you use PCI to increase value for your merchants?

Reward compliant merchants by presenting them with breach protection. When all other PCI security protocols have been followed to the best of a merchant's ability, breach protection exists to address the financial hardships a business might endure in the aftermath of a compromise. Offering breach protection will extend an olive branch and help your merchants understand you don't expect them to be perfect.

Also, make sure merchants have access to a complete set of compliance implementation tools such as internal scanning, employee training, security policies, and card data discovery. Being a complete solution provider makes it easier for your merchants because they won't have to shop around.

How much handholding does one merchant need to become PCI compliant?

Let me share with you the average number of interactions a merchant has with a SecurityMetrics support agent before they become compliant. Keep in mind, these numbers are totally dependent on a merchant's requirements, motivation, and access to internal IT staff.

I've seen as many as 20 support interactions per year, and as few as 1. The average merchant who needs SAQ assistance usually achieves compliance in one 9-minute phone call with a SecurityMetrics support agent. If the merchant is working on external vulnerability scans, it usually takes two 10-minute phone calls to get their scans into compliance, then a short call each quarter to follow-up on quarterly scans. There are also merchants who require hours of technical explanation each quarter because they have no previous technical knowledge, and no in-house IT staff to assist them.

> *Offering breach protection will extend an olive branch and help your merchants understand you don't expect them to be perfect.*

Merchants already have a difficult time understanding the value of PCI. A support staff that will hold a merchant's hand through PCI 3.0 changes would be extremely valuable.

What's the biggest security trial in processing's future?

Mobile processing security (or the lack thereof) has all but slid away from the spotlight. The industry is moving on, with mobile payments declared 'encrypted and secure'. Unfortunately, there is much to be done before a secure mobile environment can be claimed.

Mobile processing is much too convenient to slow down anytime soon. If acquirers and ISOs are determined to provide mobile solutions, it is their responsibility to educate merchants, ensure the security of the solution, and ensure the merchant knows the risk they're taking upon themselves. I suggest ISOs implement a supplemental mobile software solution to ensure basic mobile security principles in addition to any white-labeled mobile POS systems.

What necessary steps are required to ensure PCI compliance is maintained?

PCI compliance isn't a one-and-done occurrence. It's an ongoing process. Not just annually, but regularly. The trick is to convince your merchants of that. The best way to keep security on the forefront of a merchant's mind is by including it in every customer interaction and communication. Offer webinars that feature a new security topic every month, and consider offering incentives to attendees. If a significant POS update occurs, send an email prompting the update.

What is the future of PCI and security?

The future is already here. Point-to-Point Encryption (P2PE) is the most secure and liability reducing payment technology available to businesses today. If P2PE is the merchant's exclusive method of processing, it completely negates the need for network segmentation, firewalls, log management, IT personnel, etc. It's the closest a merchant can get to one-stop shop PCI compliance, likely leading to a significant diminishment of merchant PCI frustration.

Is P2PE the silver bullet? No. After all, the system can only be applied to card present transactions. However, PCI Council certified P2PE solutions relieve a significant portion of the security burden. Because credit card data is encrypted at swipe and merchants have no access to decryption keys, scope and risk are *significantly* reduced. ■