



Who's Your SECURITY GUARD?

An ISO's strategic approach to finding the right partner

By Julie Ritzer Ross

KEY NOTES

- ▶▶ Rather than search the Internet for consultants—which may yield unreliable results—ISOs should ask their sponsoring banks for a list of references.
- ▶▶ Next, ISOs must determine whether the consulting company has experience with the type of merchants in their portfolio, and to what extent they are familiar with that market.
- ▶▶ Because QSA is not a credential, ISOs should also ensure that their consulting partners are CISSP, CISA, CPISM certified.

Although ISOs are responsible for ensuring the merchants they serve process transactions securely and adhere to the Payment Card Industry Data Security Standard (PCI DSS), most need to partner with a security consultant to help them do so. But not all consultants are created equal, and a strategic approach to finding and hiring the right partner is critical to achieving best results.

ISOs can start by looking at the specific requirements for hiring a security consultant as well as the benefits of doing so. On the PCI DSS compliance front, Level 1 merchants and Level 1 and Level 2 service providers must use a certified Qualified Security Assessor (QSA) to conduct their annual on-site data security assessments. Internal audit groups can perform on-site assessments, but an officer of the company must sign off on the results. Level 2, Level 3, and Level 4 merchants, as well as Level 3 service providers, can use the PCI Self-Assessment Questionnaire (SAQ) to self-certify.

Yet despite any loopholes that may render partnering with a security consultant an option rather than a requirement, investing in the services of an expert may be the wisest choice. “Too many ISOs have been convinced that completing a SAQ and scan will protect them from fines, fees, and penalties—only to have ostensibly ‘compliant’ merchants experience data exposure incidents,” says Chris A. Mark, president of The Aegenis Group Inc., a security consulting firm headquartered in Park City, Utah. “It is important for ISOs to consider the use of consultants, as their core competencies generally do not include security and compliance.” Moreover, Mark notes, “employing skilled consultants enables ISOs to navigate the choppy waters of compliance without diverting attention from their core business.”

Where to Look

Once ISOs comprehend the wisdom of teaming up with security consultants, the temptation to simply troll the Internet in

search of prospects may be great. But don't do it.

"In the currently hot industry of information security and compliance, there are a number of self-professed 'experts,'" Mark observes. "A quick search on a major search engine will demonstrate how pervasive the practice of calling oneself an 'expert', has become. Other sources are better bets."

ISOs might start by asking their sponsoring bank for a list of references. All sponsoring banks have at least a certain degree of familiarity with security consultants, and may have a preference as to which experts ISOs use. Some also maintain lists of consultants they would prefer their ISO partners to avoid, observes Marilyn Kilcrease, president of Temecula, California-based Creative Card Solutions LLC.

Kilcrease, whose company assists financial institutions and ISOs with compliance issues, also suggests soliciting recommendations from payment networks. The latter will usually supply ISOs with a few names of third-party firms with which they have worked on network security matters.

Criteria and Credentials

Additionally, no matter what their source, prospective hires should be subjected to close scrutiny. The first—and most important—question ISOs must ask is whether the consulting entity and its associates have experience with the type of merchants in the ISO's portfolio, and to what extent the consultant is familiar with that market.

"Different verticals have very specialized needs and issues that impact data security," says Branden Williams, director of the PCI practice at VeriSign. "If the consultant being considered has had no exposure to those needs and issues, it will be difficult, if not impossible, for him or her to complete the job properly."

Williams cites the petroleum and travel verticals as examples of segments for which experience is absolutely critical. Many merchants in the former category still utilize older fuel dispensers and payment applications that require a high degree of market-specific expertise to render them capable of secure data handling, he

"Different verticals have **VERY SPECIALIZED NEEDS and issues that impact data security."**

**—Branden Williams,
director of the
PCI practice, VeriSign**

notes. Meanwhile, travel industry players retain payment information until travel is completed, with many attempting to store authentication data. This sets their security needs apart from those of merchants in other verticals, Williams explains.

Mark corroborates Williams' comments, noting that in training more than 10,000 individuals on the PCI DSS over the last two years, he and his colleagues have learned quite a bit about "good consultants and not-so-good consultants." He advises ISOs to check references to ensure consultants in question truly have a deep understanding and demonstrated experience in compliance standards like PCI DSS and also general data security. More importantly, candidates should have a track record of having provided advice that is consistent with the business as a whole and addresses the unique constraints within the industry, Mark advises.

Last year, while Mark was training merchants for a card brand, a merchant informed him that it was going to be prohibited by its QSA from accepting CVV2 data. The consultant had told the client that the risk of accepting CVV2 was simply too great, given the sensitivity of that informa-

tion. "Clearly, this QSA not only overstepped its role, but the example demonstrates a fundamental lack of understanding about the industry. The problem could have been avoided had the merchant done a more effective investigation of the QSA prior to agreeing to a hire."

Consultants' ability to be proactive also merits assessment, according to Susan Kohl, a partner at ThoughtKey Inc., an Atlanta-based consulting firm that offers PCI key/PIN management and data security program consulting services across the financial services industry. "ISOs want to work with a consultant whose method of operation involves not only dealing with the data security situation at hand, but putting in place a plan to maintain data security well beyond PCI DSS and that will come back to them with ideas down the road," Kohl asserts.

What credentials should ISOs seek in a security consultant? Credentials are less important than relevant experience in deciding whether or not to employ a particular security consultant, say experts. But some credentials do give ISOs a glimpse into a consultant's expertise. For example, the CISSP and CISA certifications are considered the de facto security certifications within information security. Additionally, the Society of Payment Security Professionals recently released the Certified Payment Card Industry Security Manager (CPISM) certification, intended to bridge the gap between information security and the needs of companies within the payment card industry.

But the QSA designation is a qualification that allows individuals to conduct PCI DSS assessment and not a credential or certification, says Mark. So when evaluating companies and individuals to support a security or compliance project, don't use the QSA qualification as the primary criterion for evaluating expertise, he says. "All in all, a more comprehensive approach will lead to better results." **TT**

Julie Ritzer Ross is a contributing writer to Transaction Trends. Reach her at juilleros@aol.com.

Security Consultants Directory

On this page are 16 companies that offer security consultation services to payments industry professionals, particularly ISOs. We've included all pertinent contact information along with a brief

description of their services and business philosophies. Be sure to check out the Web sites for the companies that pique your interest to learn more about what they have to offer.

The Aegenis Group, Inc. | Park City, UT | 435/615-6711 | www.aegenis.com

The Aegenis Group provides training, risk management, and strategic consulting in the payment card industry. It is knowledgeable with PCI DSS compliance and data security, as well as in training and market development. The Aegenis Group addresses compliance issues, and helps identify areas of residual risk in order to help mitigate exposure to breaches and reduce the likelihood of fines and penalties.

Alaric | Charlotte, NC | 704/841-7975 | www.alaric.com

Alaric supplies technology payments based products and services. It offers solutions for both SOA-based and conventional multi-channel payments integration, card authorization, switching and routing, enterprise-wide fraud detection, and card fraud detection. Products are all written in Java and fully platform independent and scalable.

Alliance Companies | Newton, MA | 617/796-8888 | www.thealliancecompany.com

Alliance Companies provide partnership development and advisory services to the payments industry. It focuses on consumer lending, portfolio assessment, and modeling, for co-branded and private label credit cards, debit cards, and credit union and agent bank card programs. Alliance Companies assist organizations with successful marketing strategies and develop consumer lending partnerships.

ArcSight | Burlington, MA | 781/685-4910 | www.arcsight.com

ArcSight offers security and compliance management solutions to identify and mitigate business risk for enterprises, MSSPs, and government agencies. It provides vendor-neutral solutions for intelligent identification, prioritization, and network response to external security attacks, insider threats, and compliance breaches. ArcSight collects details from enterprise-wide events, and supplies necessary information for organizations to make informed decisions toward protecting their company

The Authentication Authority | Sunnyvale, CA | 408/969-6100 | www.arcot.com

The Authentication Authority works to protect and verify digital identities through software-only solutions. It focuses on Internet authentication solutions for B2B and B2C portal access and online shopping applications. The Authentication Authority complies with requirements for risk-based authentication, strong authentication, e-payment, cardholder authentication, and digital signing, as well as ensures the identity of people who are accessing one's online applications.

Digital Resources Group | San Mateo, CA | 650/638-3350 | www.drsgf.com

Digital Resources Group helps merchants, service providers, point-of-sale, and acquiring institutions maneuver through the complex and changing security challenges and compliance requirements of applicable industry sectors. It offers onsite assessments, remediation, network scans, PABP validation, and penetration testing.

First National Technology Solutions | Omaha, NE | 402/633-3016 | www.fnts.com

First National Technology Solutions implements and manages company IT infrastructure in a secure environment, disaster recovery, high availability, and authorization settlement connections to Visa/MasterCard. It helps align IT infrastructures and resources with their operational and strategic business requirements. Data center and services are PCI compliant.

GSI | Kansas City, MO | 816/222-1261 | www.gsihosting.com

GSI helps to provide PCI DSS compliance, manage hosting, improve security and manage risks, help launch high-profile, Web-based promotions, and e-commerce hosting. It specializes in hosting-based solutions for businesses of all sizes and types. Apart from complex hosting, it does extensive work with data security and application delivery solutions.

Integrity Bankcard Consultants Inc. | Naperville, IL | 630/637-4010 | www.integritybankcard.net

Integrity Bankcard Consultants focus on loss prevention as a central concern in portfolio development policies, profitability analysis, underwriting standards and processes, merchant agreements, merchant risk monitoring, and ongoing merchant education. It covers the minimization, recovery, and collection of losses.

Lifelock | Tempe, AZ | 480/682-5100 | www.lifelock.com

Lifelock allows its users to take more control of who uses one's identity and how by: having credit bureaus set free fraud alerts, removing one's name from pre-approved credit card mail lists, providing free credit reports, managing card cancellations for a lost wallet, shutting down other potential identity threats, and assuring assistance in name recovery if identity is stolen.

Nubridges | Atlanta, GA | 800/251-4930 | www.nubridges.com

Nubridges offers software and managed services to protect sensitive data at rest and in transit, and to enable digital information exchange inside or outside the firewall with end-to-end security, control, and visibility. Its solutions include data protection for compliance, meeting specific PCI DSS requirements, managing trading partner community, and providing services for B2B commerce.

Panoptic Security | 801/362-8455 | www.panopticsecurity.com

Panoptic Security provides compliance solutions tailored to one's environment and business needs in order to quickly and easily comply with PCI Data Security Standard. It offers help to merchant aggregators, independent sales organizations, member service providers, and small merchants who need to take the PCI SAQ.

RSM McGladrey | Minneapolis, MN | 800/648-4030 | www.rsmmcgladrey.com

RSM McGladrey helps mid-sized companies mitigate technology-related risks. Services include PCI DSS consulting, Sarbanes-Oxley consulting, business continuity, regulatory compliance consulting, IT security and controls, as well as SAS 70 audit services offered through McGladrey & Pullen. Nearly 100 local and national offices.

Security Metrics | Orem, UT | 801/724-9600 | www.securitymetrics.com

Security Metrics offers security services including e-commerce compliance, onsite computer inspection, security policy review, internal network vulnerability assessment, penetration testing, manual computer inspection, wireless security, and war dialing. It also offers a computer security crisis response number to deal with urgent security issues.

Tarang Software Technologies | Sunnyvale, CA | 786/272-1818 | www.tarangtech.com

Tarang Software Technologies specializes in providing an array of customized solutions and services with domain expertise in payments and eLearning. It has been assessed at SEI CMM level 5, and offers time-tested advantages of offshore development backed by special delivery models. Tarang offers consultative advice on technology selection and builds frameworks to accelerate software development for clients.

Trustwave | 312/873-7500 | www.trustwave.com

Trustwave provides on-demand data security and payment card industry compliance management solutions. It assists large financial institutions to small and medium-sized retailers by managing compliance and securing network infrastructure, data communications, and critical information assets. Security consultants are CISSP-certified along with other industry technical qualifications.