

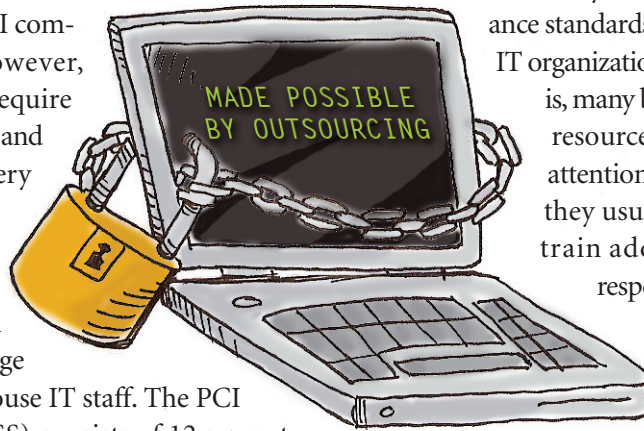
# New Compliance 'In': Outsourcing

Security breaches and identity theft are on the rise in today's network environment. According to the Identity Theft Resource Center, the number of data breaches rose nearly 50% in 2008, compromising the personal records of at least 35.7 million Americans. Knowing that a security breach can cost a business more than \$200 per record breached, smart companies are making network security and PCI compliance a top priority. However, achieving compliance can require costly and complex hardware and software installs, or at the very least maintenance and system upgrades.

Ever-evolving technology and rising breach attempts combine to challenge even the most diligent in-house IT staff. The PCI Data Security Standard (DSS) consists of 12 separate requirements made up of more than 200 individual security controls. So becoming PCI compliant is no small task. Some merchants can take anywhere from six to 18 months to accomplish their compliance objectives. To add to the complexity, the Payment Card Industry is constantly strengthening the standards for compliance and will continue to levy increasing fines and penalties on

The fact is, many businesses simply **don't have the resources** to handle the near-constant attention that **compliance** requires.

today's economy. For example, 73% of U.S. executives interviewed by PricewaterhouseCoopers said their businesses presently outsource one or more business processes to external service providers. In another survey, done by Yankelovich, 84% of company CEOs said they were satisfied with their outsourcing experiences.



merchants who fail to reach compliance. With that in mind, many companies are taking advantage of one of the fastest-growing business strategies available today: outsourcing.

Recent surveys confirm that most successful businesses are taking advantage of outsourcing in

## Bring in the Experts

Outsourcing is a quick and cost-effective way to achieve PCI compliance without affecting the IT organization's support of day-to-day operations. Attempting to take care of compliance in-house typically results in issues beyond the expertise of staff resources. It is also up to the same staff to stay on top of the industry and compliance standards and deadlines. Also, merchant IT organizations are not staffed 24/7. The fact is, many businesses simply don't have the resources to handle the near-constant attention that compliance requires. And they usually cannot afford to hire and train additional staff to take on this responsibility. Even hiring staff dedicated to compliance has its risks: Estimates put the costs of turnover at around 75% of an employee's salary.

Outsourcing to a managed service provider both alleviates these hurdles and significantly reduces the time it takes to become compliant. Because a quality-managed service provider serves many customers, it can justify investing in industry-leading, best-in-class tools and solutions. Consequently, a business can take advantage of the resources and superior skill sets of the outsourced provider. A business can also expect efficiency improvements by outsourcing its PCI-compliance initiative because managed service providers can offer solutions, as well as audited compliance, much more quickly than in-house efforts.

Working with an external provider for compliance helps reduce business risk. A company skilled in security and compliance solutions can work with a merchant organization to reduce its overall risk profile for cardholder information as well as all other sensitive information within the environment. Traditional security-solutions providers have typically focused on larger enterprises. As such, their monthly price for compliance services can be well into the hundreds or even thousands of dollars per location. Thankfully, a few innovative providers are now tailoring integrated security and network solutions for PCI compliance specifically for c-store environments. These packages can range in cost from as low as \$20 to \$150 per month per location.

**How to Begin**

Assistance from external organizations can be used for specific isolated issues or for a complete program beginning with initial assessment and continuing to ongoing operations. Either way, the starting point is always assessment. Unless the merchant is permitted to submit a self-assessment, a Qualified Security Assessor (QSA) performs the audit of the merchant cardholder data environment against the PCI DSS. This assessment identifies items of noncompliance, which can then be addressed to achieve compliance. Usually, it is at this point that a merchant chooses to bring in the experts. Firms ranging from network solutions providers to Managed Security Service Providers (MSSPs) can help with the design and implementation of specific solutions. Beyond the systems, outsourcing to these organizations can provide ongoing managed security and network services to monitor, manage and maintain the merchant’s cardholder data environment. These services typically provide support from a 24/7 security operations center and include the logging, reporting and archiving of security data required by the PCI DSS.

**Finding the Right Help**

When selecting a managed service provider, the first thing to do is confirm the provider is certified as PCI compliant.

Verification can be done online at Visa’s website ([www.visa.com](http://www.visa.com); search for PCI compliant service providers). Then the business should take the time to find a provider that has the knowledge, experience and flexibility

**A company skilled in security and compliance solutions can work with a merchant organization to reduce its overall risk profile for cardholder information as well as all other sensitive information within the environment.**

to keep the business compliant while it grows, always keeping management well informed.

Also keep in mind that although compliance follows a standard, each business is different and a provider should be able to tailor an outsourcing solution that fits its potential customer’s business model. Finding a provider that can

structure its services to meet both current and future business needs is important. As with any significant investment in a service provider, ask for client references—ideally, those in similar businesses.

**A Continuous Process**

Because audits are simply a snapshot in time, and true compliance is a day-to-day, hour-to-hour job, outsourcing to a managed service provider can prove to be the smartest, safest and most cost-effective path to sustainable PCI compliance and security. Outsourcing provides current generation, industry-leading solutions, coupled with the deep subject-matter expertise of dedicated security professionals. In today’s environment, it’s one example of a simpler solution to a complex problem that benefits both merchants and their customers alike. ■



**Dan Glennon** is the senior vice president of marketing and strategy at Cybera Inc., a leading provider of managed security and network services. Cybera’s solutions integrate all enterprise applications including private intranet, voice-over IP, credit/debit transaction processing, public Wi-Fi hotspots, IP video, and many other applications with a single managed security and network solution that meets the strict regulatory requirements of Sarbanes-Oxley, PCI-DSS and HIPAA. Contact him at (866) 4CYBERA or visit the Cybera Web site at [www.Cybera.net](http://www.Cybera.net).



**Maurice P. Minno** is president of the MPM Consulting Group and a partner of ISUS (Inventive Strategies and Unique Solutions). Operating with strategic partners such as Cybera, the MPM Group provides cost effective, holistic PCI compliance and connectivity option solutions. Contact him at (760) 250-7791 or visit the MPM Group Web site at [www.MPMGroup.net](http://www.MPMGroup.net).