

contents

Strategies for PCI compliance

- 2 Requirement 6.6
- 7 Choosing an assessor
- 11 Compensating controls
- Outsourcing**

Mastering PCI

Compliance with the Payment Card Industry Data Security Standard requires intimate knowledge of the regulation and your organization's environment.

BY INFORMATION SECURITY AND SEARCHSECURITY.COM

SPONSORED BY



FIBERLINK



solidcore



utimaco
The Data Security Company.

PCI 6.6 shines light on shoddy coding

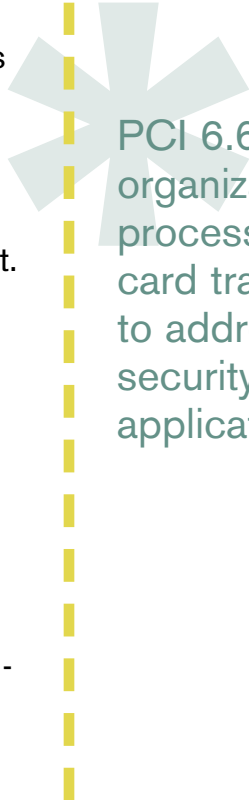
BY MICHAEL S. MIMOSO

Now a requirement, 6.6 puts several important choices in front of organizations.

Say one thing for the PCI Security Standards Council: They've got great timing. Requirement 6.6 of the Payment Card Industry Data Security Standard, which became mandatory on June 30 and governs the security of Web-based applications, arrived on the heels of one of the worst blind SQL injection attacks on record. Those coinciding events made evident the glaring security shortcomings in Web applications, and the lengths attackers will go to in order to target enterprise data.

PCI 6.6 requires organizations that process credit card transactions to address the security of Web applications, either via manual or automated source code reviews or vulnerability scans, or via the installation of a Web application firewall (WAF) between a Web app and the client endpoint.

For the 18 months prior to June 30, 6.6 was a best practice. Now, many organizations are acting like high-schoolers cramming the night before a final exam, having devoted only marginal attention to compliance to date; experts unanimously say compliance is low despite a solid level of awareness. The PCI Security Standards Council is partially to blame; the requirement was ambiguous as to whether organizations were required to conduct a source code review and install a WAF. A clarification was ultimately issued in late April that



PCI 6.6 requires organizations that process credit card transactions to address the security of Web applications.

said either or would satisfy the intent of the requirement.

In the meantime, attacks on Web applications intensified and matured. April's shotgun-style SQL injection attack that compromised thousands of websites established a new frontier of trouble for Web applications.

Applications have been the attack vector of choice for some time, but recently, hackers have moved away from traditional SQL attacks that compromise individual websites. Instead, working from lists of vulnerable PHP and ASP web pages compiled from search engine queries, hackers based mostly in China have figured out how to scale their attacks and improve their odds for success.

Frightening not only for its scale, but its effectiveness in injecting malicious code into database tables, organizations, in many cases, are hopelessly behind the eight-ball as a result of these attacks. Cleanup is close to impossible because a DBA would either have to scour a database row by row and table by table to find the code and remove it, or restore a database from a recent backup—if they have one. Essentially, infected databases have been backdoored via a Web application, and even if the initial

payload is benign, it can be swapped out at any time.

CHECKMARK CHALLENGE

Compliance with PCI 6.6, in the end, likely won't help against this particular attack, but it is a wake-up call for organizations to address the code they build or customize. In the meantime, auditors may show some mercy with early assessments, but that leniency won't last for long. This is especially bad news for smaller merchants, Level 3 and 4, who don't have the resources or expertise to either adequately review source code, or purchase and properly configure a Web application firewall.

Manual source code reviews are extremely expensive and time consuming. Automated vulnerability scans are less so, but still tax the bottom line. Web app firewalls, meanwhile, are likely the quickest way to a compliance checkmark, and some experts say this is a fitting starting point until an organization matures sufficiently to tackle its proprietary code.

“Many organizations start with a Web application firewall to get a checkmark. That is not necessarily raising the bar in terms of security, but they would be meeting the compliance factor,” says Danny

“Many organizations start with a Web application firewall to get a checkmark. That is not necessarily raising the bar in terms of security, but they would be meeting the compliance factor.”

—Danny Allan, director of security research, IBM Rational

Allan, director of security research with IBM Rational.

Allan points out that organizations should want to do both, but the most likely scenario is one where an organization grapples with how to compare the two options afforded by 6.6 and deciding which is the best immediate fit.

“There’s no right answer,” Allan says. “Some recommend beginning with a Web application firewall, but a WAF needs to be configured properly to work. If you’re in a fluid environment [one where applications change and grow in complexity], that can require a fair amount of time to configure. And ultimately, you’re putting a Band-Aid on the issue. The application still has the problem.”

WAFS THE QUICKER ROUTE

Web application firewalls, also known as deep-packet inspection firewalls, look at application layer messages for violations of an established security policy. Some offer signature-based protection, while others are fed a baseline of appropriate application behaviors and monitor for deviations. They’re offered either as software or in an appliance. WAFs struggle detecting certain types of attacks because they don’t always under-

stand the context under which input is entered into an application, and legitimate traffic could be dropped if a WAF believes the traffic violates policy. Also, some tools fail to detect some serious Web app threats such as cross-site scripting attacks.

“In my mind, you want to do both [6.6 options], but this is an apples to oranges comparison,” Allan says. “Which gives you more of a bang in the short term? That is the question that needs to be answered.”

Therefore, WAF sales are bound to see a bump in the coming 12 months.

“Smaller merchants are going to gravitate toward a WAF if it will get them a checkmark,” says David Taylor, founder of the PCI Knowledge Base and research director of the PCI Security Vendor Alliance. “That is where things are going. It’s not wrong; it’s the most cost-effective way to go. I would never tell a Level 3 or 4 merchant to spend more money than they have to.”

SECURE CODING

Source code reviews, meanwhile, are the ideal solution, experts say. For some time, experts have urged organizations to include security in the software development life-cycle. Automated scanners can test appli-

“Smaller merchants are going to gravitate toward a WAF if it will get them a checkmark.”

—David Taylor, founder, PCI Knowledge Base and research director, PCI Security Vendor Alliance

cations for vulnerabilities, in particular the Open Web Application Security Project (OWASP) top 10 list of flaws. In fact, PCI DSS 6.5 says Web applications should be developed based on guidelines such as OWASP and applications should be secured against the vulnerabilities listed in the top 10, which is updated annually.

But developers generally shun security because it hampers productivity and functionality. Manual reviews are difficult, though sometimes they're essential in order to catch problems in the context of an application's semantics. Expense aside, manual reviews require inspection, often of hundreds of thousands of lines of code, and it's virtually impossible to follow all the logic paths an application can take, says Barmak Meftah, senior VP of products and services at Fortify, a vendor of static and dynamic source code analysis tools.

"The main type of vulnerability a hacker is getting hold of is an input field—putting in malformed input and getting the app to do unintended things," he explains. "That packet is now using different paths than intended, and connecting those dots optically is impossible."

The big picture is that organizations don't look at 6.6, and source code reviews and the

use of automated scanning tools and the deployment of a Web application firewall in the context of an overall vulnerability management program, says IBM Rational's Allan.

"Security threats are changing daily. PCI 6.6 is a strategic approach: How do I address this fluid, changing paradigm of security attacks that is going to be different tomorrow than today?" Allan says. "This is about building good, quality code. If we keep focusing on the security aspect and not building quality apps, we're forever going to be chasing security vulnerabilities."

Allan and other experts, however, concede that's an idealistic view. For the meantime, organizations bound by PCI are going to do what it takes to get a checkmark, and think compliance first, security second.

"Web application firewalls are not going to stop all attacks. The same thing is true for source code reviews; someone needs detailed knowledge of the business logic to do and appropriate review," says Sumedh Thakar, PCI solutions manager at Qualys. "Neither one seems to be perfect solution. It definitely comes down to the resources people have. The ideal way is to do everything. Do source code reviews as part of your software development lifecycle. Do

"Web application firewalls are not going to stop all attacks. The same thing is true for source code reviews; someone needs detailed knowledge of the business logic to do and appropriate review."

—Sumedh Thakar,
PCI solutions manager,
Qualys

testing on a running app with automated tools. Have a WAF in place to trap what it can, and on an ongoing basis, use automated tools to do additional pen-testing.”*

Michael S. Mimoso is editor of *Information Security*.

PCI 6.6

PCI 6.6 reads as follows:

Ensure that all Web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.
- Installing an application-layer firewall in front of Web-facing applications.

The audit procedures for 6.6 read as follows:

- Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections.
- Verify that an application-layer firewall is in place in front of Web-facing applications to detect and prevent Web-based attacks. ▶

Choose your QSA wisely

BY MARCIA SAVAGE

PCI assessors stand between you and compliance. Ensure your assessor is a match to your organization's needs.

Organizations looking for a PCI assessor should do some homework ahead of time to ensure they choose the one who best suits their needs. Don't rush to hire an assessor without first digging into their background, experience and compliance philosophy, experts advise.

"Blindly going at it is probably the wrong approach," says Randall Gamby, analyst at research and consulting firm Burton Group.

Organizations bound to PCI, such as large merchants and service providers, work with Qualified Security Assessors. The PCI Security Standards Council governs training

and approval of QSAs, who issue the Report on Compliance to acquiring banks and card brands.

Just as a company checks out the background of employee candidates, it should delve into the background of potential assessors. Find out their level of technical expertise and whether they've been internal auditors, system administrators or network architects, says Dave Shackleford, director of Configuresoft's Center For Policy & Compliance. And get references.

"A lot of people don't dig that deeply," he says.

MATCH EXPERIENCE AND INDUSTRY

When reviewing an assessor's background, it's important to look at what industries he or she has worked in. If a manufacturer taps a PCI assessor that has specialized in financial services, there may not be a "one-to-one match in the kind of methodology" the firm uses, Gamby says.

"Make sure the person in question knows

Don't rush to hire an assessor without first digging into their background, experience and compliance philosophy, experts advise.

your industry,” says David Taylor, founder of the PCI Knowledge Base and research director at the PCI Security Vendor Alliance. He adds that he’s seen complete mismatches, such as a retailer audited by a specialist from the aerospace industry who decided to try his hand at security.

Another consideration is the assessor’s location, says Troy Leach, technical director at the PCI Security Standards Council. A global organization might find it more expensive to hire an assessment firm that operates only in North America; a company that operates in multiple countries needs a firm that can handle audits and understand the language in those countries.

It’s also important to check the experience of the individual assessors working at an assessment firm to avoid any surprises. “Who is actually going to do the review? Is it Joe fresh out of college, or Mary who has been doing this for 10 years?” Taylor says.

While Taylor acknowledges that QSA firms can’t control employee turnover, he recommended that companies get some assurance about the level of staff expertise, even if the firm can’t guarantee a particular assessor. QSAs must be certified by the PCI Security Standards Council; organiza-

tions can also ask if a QSA holds certifications such as the CISSP, CISA and Certified Internal Auditor.

In April, the PCI Security Standards Council launched a database of individual QSAs. Companies can go to the council’s website <https://www.pcisecuritystandards.org/> and look up assessors by their name, certificate number and their company to verify that they are currently certified. Leach says merchants need to know the name of the assessor to search the database but the council planned to add new features that will allow a search by company.

The council’s website is a good place to start looking for an assessor. Gamby suggested that organizations could also check with their internal audit and compliance departments for referrals. “Most large organizations have a compliance or audit group. See if they have someone to start with. It might make sense from an overall security posture to have the same auditor.”

TWO QSAs BETTER THAN ONE

But before starting a search for a QSA, a company should conduct an analysis of its environment, Leach says. Knowing what systems contain cardholder information will

QSAs must be certified by the PCI Security Standards Council; organizations can also ask if a QSA holds certifications such as the CISSP, CISA and Certified Internal Auditor.

reduce the cost of the assessment because the assessor will have less leg work, he says. Also, the analysis may reveal cardholder data residing on unique or archaic technologies such as mainframes. Armed with that knowledge, a merchant can screen assessor candidates based on whether they have experience with those technologies.

“Having an assessor who is familiar with everything in your environment, your technology and your industry, would be very helpful so they can hit the ground running,” Leach says.

Some companies opt to hire two QSAs, one to perform a gap analysis, also referred to as pre-assessment or remediation work, and another for the validation work. Companies need to take into account the type of work they want performed when looking for a QSA, Gamby says: “The No. 1 thing to understand is what you want to get out of a PCI assessment.”

The reason for having two QSAs can be compared to someone not going to the Internal Revenue Service to see if he has issues with his tax return, he says. Organizations often go with two assessors in order to prepare for the audit and to get an unbiased opinion for it. “The person who audits you shouldn’t do your gap analysis,” he said.

COMPENSATING CONTROLS

Whether an organization hires one or two assessors, it should make sure whomever they tap shares its philosophy about compensating controls, Taylor says.

“If a company has known problems relative to certain areas related to compliance, and they choose an assessor with a strict no compensating controls policy, then they’re going to set themselves up to pay a heck of a lot of money,” he says.

Assessors who come from an accounting background tend to be characterized as “harder graders,” he adds.

Taylor also advises checking an assessor’s policy on documentation. “Some companies charge a lot for that documentation, others almost give it away. Understand the documentation, and their process for creating and reviewing it,” Taylor says.

He has seen cases in which assessors conduct multiple interviews at an organization in the course of a PCI review, yet tell the organization they’re not convinced it is compliant. So it’s important to have an agreement about the criteria for compliance and the types of tests they’ll be performing, he says.

Gamby says some assessors come from a

“If a company has known problems relative to certain areas related to compliance, and they choose an assessor with a strict no compensating controls policy, then they’re going to set themselves up to pay a heck of a lot of money.”

—David Taylor, founder, PCI Knowledge Base and research director at the PCI Security Vendor Alliance

technology perspective while others are more process oriented, and that organizations need to understand which approach a prospective assessor uses.

A technology-focused assessor may look for a Web application firewall when it comes to PCI DSS Requirement 6.6 while a process-oriented will look more closely at the software development lifecycle, he says.

PCI 6.6 requires organizations to address the security of Web applications, either via manual or automated source code reviews or vulnerability scans, or via the installation of a Web application firewall (WAF) between a Web app and the client endpoint. PCI 6.6 became a requirement on June 30.

“Some just use what I consider common sense. Others are looking to check off boxes,” he says. “So you really have to understand what kind you’re working with.

Configuresoft’s Shackleford warned that some large assessment firms rely on checklists as they churn out PCI reviews, and have built reputations for validating organizations as compliant.

Companies shouldn’t consider volume of work as a top consideration when choosing an assessor, he says.

“At the end of the day, you’re left wonder-

ing, ‘Did I really pass muster, or did they just want to get out of here and give us the check box to sign and move on?’ ” Shackleford says. “Volume isn’t necessarily the most applicable factor. It’s the quality of the work, similarity across verticals and backgrounds of the teams.”

Shopping around for a cheap deal isn’t the best strategy in looking for a PCI assessor, says Ken Smith, principal security consultant for IT solution provider Akibia. He says it’s unnerving to see some assessment firms working so quickly and cheaply.

Shackleford says PCI assessments range in cost, anywhere from \$10,000 to \$500,000. Usually they involve a two- to four-week preparation phase, in which documentation is exchanged, and an onsite phase of two to three weeks. Some organizations with a lot of sites that require travel may take up to six weeks for the onsite portion.

“You get what you pay for,” he says. “If someone comes in and says they’re going to do the whole thing in two weeks, it should raise red flags.”*

Marcia Savage is features editor of *Information Security*.

“Some just use what I consider common sense. Others are looking to check off boxes. So you really have to understand what kind you’re working with.”

—Randall Gamby,
analyst, Burton Group

Loophole or life-saver: Compensating controls

BY DENNIS FISHER AND ROBERT WESTERVELT

Compensating controls enable organizations to meet the intent of PCI requirements without breaking business processes—or the bank.

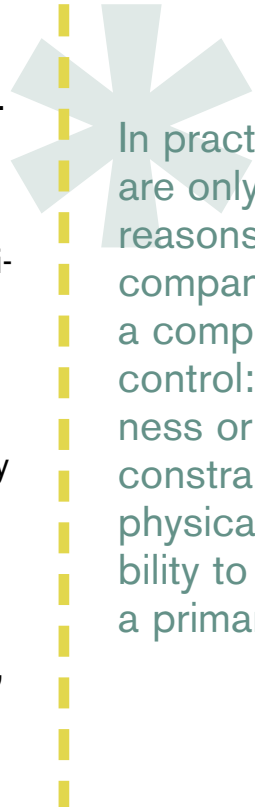
As compliance with the Payment Card Industry Data Security Standard (PCI DSS) has become more complex, an increasing number of businesses rely on compensating controls to satisfy requirements they'd otherwise have no way of meeting.

Designed to enable companies to comply with the spirit and intent of the requirements, compensating controls have also become something of a hot-button issue as some

assessors question whether organizations are using them as a loophole when a control is otherwise too costly to implement. Although, version 1.1 of PCI DSS, released in 2006, somewhat closed the loophole when the council declared compensating controls could not be used unless an organization had already failed one assessment.

In practice, there are only two reasons for a company to use a compensating control: a business or technical constraint, or a physical impossibility to implement a primary control. For example, a retailer with 5,000 locations would have a physical problem deploying encryption on all its legacy point of sale systems resulting in the use of a compensating control, says James DeLuccia, a PCI expert and author of *IT Compliance and Controls*.

But some companies need to do a better



In practice, there are only two reasons for a company to use a compensating control: a business or technical constraint, or a physical impossibility to implement a primary control.

job understanding the intent of the primary control before deploying something else and calling it a compensating control. Often, they fail to provide good documentation described in the compensating controls worksheet that identifies and supports how the cardholder data will be protected using a different method, DeLuccia says.

COMPLIANCE CHECKLIST

Companies should begin by identifying the issues that may preclude compliance with the requirement, DeLuccia says. Then define the objective being met by the compensating control and conduct a risk analysis to determine any additional risks. Test, document and explain how the compensating control meets the objective. The explanation should address how the compensating control meets the original objective and the identified expanded risks, DeLuccia says.

“PCI requires seven-character passwords. Some people have mainframes that don’t allow passwords longer than six characters, so you automatically can’t satisfy that without replacing the mainframe,” says Michael Gavin, a security strategist at Security Innovation and a Qualified Security Assessor (QSA). “A compensating control is if you

can force all connections to go through an authentication phase before the password. That meets the requirement.”

The current process for an assessor to approve PCI compensating controls introduces potential problems. Organizations may change auditors year after year, so a level of uncertainty exists in the acceptance of these controls, DeLuccia says. Also, it is in the auditor’s interest to accept the compensating control, because he serves the client and has an incentive to accept it. Finally, DeLuccia says compensating controls require more mature control environments. This could mean additional processes and technologies to fully address the risk.

“A common mistake is thinking that compensating controls are temporary—not necessarily. They may remain in place so long as they satisfy the risk appropriately,” DeLuccia says.

DON'T FORGET DOCUMENTATION

In recent months, the PCI Standards Council has addressed the methodology of determining and documenting compensating controls and that is creating better transparency. This is better for everyone involved because it protects the QSA from

“A common mistake is thinking that compensating controls are temporary—not necessarily. They may remain in place so long as they satisfy the risk appropriately.”

—James DeLuccia,
PCI expert and author of
*IT Compliance and
Controls*

accepting a set of compensating controls with less risk, while ensuring payment operators are not singled out and penalized unnecessarily, DeLuccia says.

Roger Nebel, an independent PCI DSS auditor and director of strategic security at FTI Consulting, agrees that PCI compensating controls should be chosen very carefully and always be well-documented. The company should understand the strength of the primary control and what it's intended to do. Once implemented, an assessor has to evaluate whether the compensating control meets the objective of the primary control and whether other entry points are opened to the sensitive data, Nebel says.

Still, whether a compensating control passes muster will be up to each individual assessor and ultimately the strength of the organization's documentation.

"They certainly need to be reviewed every year. As long as you are meeting the intent of the requirement as stated, it's normally OK," says Gavin. "The real purpose is to allow people to be compliant without forcing them to buy new products. If you have to be compliant, meeting the letter could cost you a fortune and the controls are an acknowledgement that people were doing security

before and maybe what they were doing was good enough and can be augmented."

The PCI Security Standards Council is trying to address the inconsistencies among QSAs. It's developing a training program and an assessor evaluation program. An assessment team appointed by the council will evaluate feedback from merchants on assessors. Negative feedback could result in probation and revocation process for assessors.

The PCI Security Standards Council is likely to address ineffective compensating controls in the next release of the standard due in October. Experts say that as the standard evolves, the use of compensating controls will become less clouded.

Although it's not an official compensating control, Nebel points out that network segmentation is one form of a compensating control. Segmenting shouldn't be taken lightly, he says. Sometimes company executives believe they have segmented off the cardholder data, but the QSA discovers entry points to the main network.

"You're narrowing down the scope of the systems you're going to look at," Nebel says. "You're isolating the cardholder data from normal network activity either through a

The PCI Security Standards Council is likely to address ineffective compensating controls in the next release of the standard due in October.

VLAN or a firewall.”

Nebel evaluated a service provider that claimed its cardholder environment was segmented. But after reviewing the documentation and assessing the controls in place, Nebel found that the environment could be accessed administratively from certain workstations.

“There’s a whole set of controls for remote management that requires communications to be encrypted and two-factor authentication,” Nebel says. “They thought everything was fine, but it wasn’t.”

While network segmentation helps reduce the scope of a project, other areas, including PCI requirement 6.6, could be an area where compensating controls help meet the requirement, says Mike Rothman, president and principal analyst of Security Incite. PCI requirement 6.6 gives two options for protecting Web applications—application code reviews and Web application firewalls. For the best protection, the PCI Security Standards Council recommends using both methods. But securing Web applications is difficult and while some organizations could look at Web application firewalls as the answer, others will look for alternatives to satisfy the requirement, Rothman says.

“When an in-depth code review or alternative measures may not be feasible, some folks may try to get creative,” Rothman says.

ASSESSOR HAS FINAL SAY

Rothman agrees that ultimately the success or failure of implementing a compensating control will come down to the judgment and experience of the assessor. A company that has its credit card data protected by several layers of security and can only be accessed by an internal person with the proper administrative controls will likely meet the encryption requirement via a compensating control, but it will all come down to the assessor’s judgment, Rothman says.

“It’s up to the experience and capabilities of the assessor to really distinguish whether a compensating control really does solve the problem,” he says. “Companies will still want to go through the process and look at it from an attack vector standpoint and ensure that nothing was missed.”

There are no generic answers—every company has a slightly different environment around credit card transaction systems—so that’s why compensating controls are unacceptable for the first assessment, Rothman says. The PCI Data Security Standard lays

“It’s up to the experience and capabilities of the assessor to really distinguish whether a compensating control really does solve the problem.”

—Mike Rothman, president
and principal analyst,
Security Incite

that out, saying that companies should be aware that a particular compensating control will not be effective in all environments.

“I look at everything with a skeptical eye. As a QSA, I have to look for weaknesses and make sure things are implemented and managed properly. Is this control adequate? Does it meet the requirement?” Gavin says. “To me, the intent is to improve everyone’s security to a certain level. If it’s cheaper, that’s OK.”*

Dennis Fisher is executive editor of TechTarget’s security media group. Robert Westervelt is news editor of SearchSecurity.com.

DEFINITION

Compensating controls

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

Compensating controls must:

- 1) Meet the intent and rigor of the original stated PCI DSS requirement;
- 2) Repel a compromise attempt with similar force;
- 3) Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

SOURCE: PCI DSS v1.1 glossary

Outsourcing is a slippery compliance slope

BY MARCIA SAVAGE

Providers are required to be compliant with PCI, but that doesn't liberate merchants from liability in the event of a breach.

Your organization may be PCI compliant, but is the company it outsources to? Outsourcing has become a hot topic in the world of PCI compliance as more organizations, including smaller merchants, grapple with the payment card industry's standard for keeping cardholder data secure. With those smaller merchants likely to outsource some credit card processing functions, the topic has taken center stage, says Dave Shackelford, director of Configuresoft's Center For Policy & Compliance.

"The bottom line is any third party that's handling the data has to be just as compliant as you do. Period," he says.

Companies that share cardholder data with service providers are obligated to contractually require that the service provider adhere to PCI Data Security Standard requirements.

"If you have a service provider that will be dealing with cardholder data, you have an obligation in your contract to say they must be PCI compliant and an obligation to actually validate where they are in compliance," says Phil Cox, principal consultant at security consulting firm SystemExperts.

Companies typically obtain a SAS 70, which usually satisfies PCI auditors, Shackelford said. In some cases, though, they may require a specific PCI audit of the third party. Before engaging in outsourcing activities, companies should consult with their acquiring banks, Shackelford advises. The acquir-

"If you have a service provider that will be dealing with cardholder data, you have an obligation in your contract to say they must be PCI compliant and an obligation to actually validate where they are in compliance."

—Phil Cox, principal security consultant, SystemExperts

ing bank is ultimately the liable party in the event of a breach, and the banks differ in their requirements, he says.

“See how they would like to proceed on getting a third-party, objective audit of the outsourced environment,” he says.

ALL OR NONE

At the same time, however, companies can reduce the scope of their PCI requirements by outsourcing all payment card processing functions—a trend Cox expects many in the industry will follow because it’s cheaper and quicker. “They’re moving it off and saying they’re not in the business of processing credit cards.”

By having a third party handle all transmission, storage and processing of cardholder data, a merchant will greatly reduce the scope of its PCI self-assessment, says David Taylor, founder of the PCI Knowledge Base and research director at the PCI Security Vendor Alliance “You still have to file a self-assessment questionnaire, but you can file the simple one,” he says.

Earlier this year, the PCI Security Standards Council released four new PCI self-assessment questionnaires (SAQ) that experts says are streamlining compliance

for many businesses, especially those that outsource payment card functions. In a Feb. 12 report, Avivah Litan, vice president and distinguished analyst at Gartner, says the new SAQs replaced “an unrealistic one-size-fits-all questionnaire that did not reflect the reality of card-accepting businesses’ operations and was not aligned with the PCI DSS itself.”

Litan noted that the new SAQs distinguish between e-commerce merchants that outsource all payment processing and card data storage to a PCI-compliant payment service provider and e-commerce or brick-and-mortar merchants that have payment systems that connect to the Internet but don’t store any data. She expected the new SAQ process to drive more card data outsourcing.

For example, the SAQ for organizations that outsource all cardholder data functions is very short and includes questions about the type of business and whether the third party handling cardholder data is PCI DSS compliant. The SAQ for organizations with point-of-sale systems connected to the Internet but no electronic cardholder data storage asks for confirmation that the payment application does not store sensitive authentica-

Earlier this year, the PCI Security Standards Council released four new PCI self-assessment questionnaires that experts says are streamlining compliance for many businesses, especially those that outsource payment card functions.

tion data after authorization, and whether a merchant is compliant with the 12 PCI DSS requirements. If not compliant for any of the 12, a merchant must provide a remediation plan and timeline.

DON'T BUY THE SALES PITCH

Merchants should be wary, however, of vendors who claim that outsourcing will eliminate their PCI problems, warns Ken Smith, principal security consultant for IT solution provider Akibia.

“A couple vendors have said, ‘We hold the data, so you don’t have worry about PCI anymore,’” he says. “The merchant with the online presence is ultimately responsible for taking care of their customers.”

Visa maintains a list of service providers that are PCI compliant, but places the responsibility on members to follow up with service providers with any questions about their compliance status. The PCI DSS Requirement 2.4 requires hosting providers with access to cardholder data to protect each merchant’s hosted environment and data; Appendix A specifies that hosting providers must ensure logging and assessment trails are enabled and unique to each entity’s cardholder data environment, and

must have processes to provide timely forensics investigation in the event of a breach to any hosted merchant or service provider.

Appendix A notes that a hosting provider meeting the standard’s requirements doesn’t necessarily guarantee compliance for a merchant; each entity must comply with PCI DSS.

“When you outsource, you need to make sure the company you’re doing business with is PCI compliant,” Taylor says. “You need some form, signed letter, or compliance certificate.”

Organizations should ask for the service provider’s Report on Compliance issued by its QSA, Shackelford says.

Some companies are requiring more validation and are conducting detailed evaluations and even physical visits to the third party. Some financial-services firms and large retailers send audit teams to physically inspect whether their third parties are compliant.

“If you’ve outsourced parts or all of what you’re doing from a card processing standpoint, you can’t just rely on that letter,” Taylor says. “If there’s a problem with that [outsourcing] company, your brand gets dragged through the mud.”

If there’s a problem with that [outsourcing] company, your brand gets dragged through the mud.”

—David Taylor, founder, PCI Knowledge Base and research director, PCI Security Vendor Alliance

Indeed, it's not just a matter of having a contract that requires an outsourcer to be PCI compliant, says Randall Gamby, analyst at research and consulting firm Burton Group. "You have to make sure they're willing to be audited by you and that they accept your controls on the information," he says.

Outsourcers sometimes push back on audit requests, though. "They're notorious for doing that," Shackleford says.

He recalled a sticky situation a few years ago when he was a security manager at an airline. This was before PCI DSS, but the company needed to comply with MasterCard's Site Data Protection program and like many airlines, used an outsourcer for a lot of payment card processing. The outsourced firm, however, balked at an audit.

"They were totally unwilling to let me onsite and take a look at what they had," Shackleford says.

He ended up working with security directors at four other airlines to demand, and ultimately force, the outsourcer to comply with a SAS audit of its card processing environment.

AUDIT YOUR PROVIDER

It's also important to check outsourcers' ongoing security by conducting periodic reviews and audits. Contracts should include provisions for spot checks or other types of reports, Gamby says. "You need to understand what their ongoing security strategies are. They may be PCI compliant at a point in time, but it doesn't mean they're compliant forever."

Some organizations have moved from annual audits to quarterly reviews, noted Taylor: "Compliance and security are such that the changes in your company, in your third party, in the way you communicate with the third party that you've outsourced to, can compromise your compliance and security on an almost daily basis."

In the event of a breach at an outsourcer, it's the name of the company that outsourced which customers will see on the letterhead, he says. "It's all nice and good that you've outsourced and you can reduce the scope, but you still own the problem."

For that reason, Gamby suggests that companies include language in their outsourcing contracts that provides for monetary damages if a breach occurs. While the acquiring banks are ultimately responsible

"You have to make sure they're willing to be audited by you and that they accept your controls on the information."

—Randall Gamby,
analyst, Burton Group

for the payment cards, they will likely shift costs onto the merchant who suffered the breach.*

Marcia Savage is features editor of *Information Security*.



Breach Security

Webinar: Why Security Shouldn't Take a Back Seat to PCI

Learn about the risks associated with the storage of sensitive data and how you can protect it.

The Breach Security Guide to PCI Compliance for Web Applications (Updated for PCI DSS Version 1.2)

Learn about the PCI web application security requirements and your options for compliance.

The Aegenis Group's Evaluation of Breach Security WebDefend Relative to the Payment Card Industry

Read an independent evaluation by the worldwide PCI Qualified Security Assessor (QSA) trainers.

Overstock.com Selects Breach Security WebDefend to Protect Online Customers

Breach Security safeguards Overstock.com customer credit cards and enables PCI compliance.

Stephen S. Wise Temple Chooses WebDefend for Non-Intrusive and Effective Web Application Security

Stephen S. Wise Temple achieves PCI compliance and protects its members with Breach Security.

Fiberlink

Extending PCI Compliance to the Mobile Workforce

If your laptops aren't covered neither are you. Learn how the PCI DSS requirements map to specific mobile security technologies and best practices.

Get Control of Mobile Data (and More)

Learn how to improve security and reduce costs with a mobility management platform (Video webcast).

Managing Mobility – An Introduction to Fiberlink

Protect data on mobile devices and reduce the cost of compliance, security and connectivity.

Rapid7

Using an Expert System for Deeper Vulnerability Scanning

NeXpose Unified Vulnerability Management performs accurate scanning using an expert system to achieve better results than traditional procedural methods.

Web Application Scanning—Securing Your Web Site from Malicious Intruders

Find out what a security administrator needs to know about Web applications and how to successfully protect your network from Web application vulnerabilities.

Securing Web 2.0 Applications—Closing the Door to Dangerous Visitors

Although Web 2.0 applications offer rich capabilities, Web 2.0 applications contain flaws that are hard to detect automatically, making them easier to attack.

Penetration Hurts: Best Practices to Protect Sensitive Data and Achieve PCI Compliance

With no other simple guide to securing your networks, find out how companies can use the PCI DSS as a guide and develop a network security plan that protects your IT assets.

Sentriigo

Hedgehog Enterprise

PCI DSS Solution

IT Download

White Paper: Practical Guide to Database Security and Compliance

Fulfill Audit Requirements Quickly and Efficiently.

Webcast

Solidcore

Easily and cost-effectively meet PCI requirements 1, 10 and 11

Take a tour and get a free trial of the leading file integrity monitoring and audit trail solution.

Lock down your retail POS environment

Learn why leading retailers are choosing Runtime Control as an alternative to Anti-Virus.

Trustwave discusses how to meet, sustain and go beyond PCI compliance

Leading QSA illustrates how to solve difficult file monitoring and auditing requirements.

Analyst Report—More than a fast track to PCI compliance

Analyst firm EMA highlights how best to address PCI DSS file integrity monitoring.

Continuous File Integrity Monitoring is the new approach to PCI compliance

Find out why leading retailers are adopting this real-time approach to difficult PCI requirements.

Thawte

Securing your Online Data Transfer with SSL

This white paper provides an introduction to SSL security covering the basics of how it operates and how to deploy appropriate SSL certificates.

Securing your Apache Web Server with a thawte Digital Certificate

Read this white paper and learn more about securing your Apache Web Server with thawte digital certificates.

Extended Validation (EV) SSL Certificates

This white paper details the benefits of extended validation (EV) SSL certificates and how they can help your company.

Securing your Microsoft IIS Web Server with a thawte Digital Certificate

In this guide you will find out how to test, purchase, install and use a thawte Digital Certificate on your Microsoft Internet Information Services (MS IIS) web server.

The thawte Starter PKI Program

Read this white paper and learn about the advantages and benefits of the thawte Starter PKI Program.

Tripwire

Configuration Control for Virtual and Physical Infrastructure

Download this trial software and understand the proper configuration of virtualization platforms.

What's Good for Security is Good for Operations

Learn why configuration assessment followed by change auditing is key to operational stability.

Is Virtualization Under Control?

Download this white paper and learn current opinions on security & controls for virtual servers.

Optimizing Infrastructure Control

Learn the nature of infrastructure integrity, change auditing and compliance solutions.

Utimaco

SafeGuard LeakProof Product Info

SafeGuard Enterprise Product Info

SafeGuard Configuration Product Info

Webinars

Demo SafeGuard Versions