Using PCI Scope to Lower Risks and Cost

By R. Scott Pierangelo and David Lam

This article discusses leveraging technology identified in PCI Self-Assessment Questionnaires A and P2PE to reduce the risks and costs to an organization when processing credit cards, which also subjects the organization to fewer and less onerous compliance requirements. By leveraging newer technology and risk transfer, organizations can in some cases reduce questions almost tenfold.

If you process credit cards as part of doing business, you must comply with the Payment Card Industry Data Security Standard (PCI DSS). This can be a very onerous process. However, you have options to reduce your scope by leveraging new technology. This article serves to highlight those options and give some background on the PCI-compliance process.

What is PCI compliance?

The PCI DSS is an information security standard that organizations must be compliant if they store, process, and/or transmit credit card data [6]. The standard is maintained by the PCI Council, which is comprised of the major credit card brands (America Express, Visa, Mastercard, Discover, and JCB). Based on the volume of credit cards stored, processed, and/or transmitted by an organization, an organization can be a level 4, level 3, level 2, or level 1 merchant and/or service provider (with level 1 being the highest volume). If an organization is a level 1, it must complete a level 1 assessment and a third-party qualified security assessor (QSA) must perform the assessment. For all other levels, a self-assessment questionnaire (SAQ) can be completed; QSA assistance is optional, although it is recommended.

Finding the scope

The first and most critical part of PCI compliance is finding the right scope when answering your self-assessment questionnaire. According to the PCI Security Standards Council, "The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS" [5]. Note that many large businesses do not qualify to fill out the self-assessment questionnaires, but an enormous amount of businesses do.

Scope includes systems that process, store, or transmit cardholder data or provide security services for said data and the systems the data traverses. Networks that are not segregated properly can also be in scope. For many small and medium businesses (SMBs) this means bringing into scope systems that aren't properly secured in accordance with the requirements. In a nutshell, reducing scope includes both having less systems that might handle cardholder data and not having any cardholder data to touch or store.

Interestingly enough, most businesses are not well versed in what questionnaire needs to be filled out. In fact, both of the authors have worked on situations where clients were answering over two hundred unnecessary questions and becoming compliant to those standards because the organization and their teams were not appropriately educated in what questionnaire to fill out when achieving compliance. Here are two things to consider:

- Different SAQ questionnaires meet different PCI needs.
- The number of questions range from 22 to 329 (unless you are a service provider). This means that the choices you make in implementing credit card acquisition has a significant impact on your business, both from a cost and a workflow perspective.

Now, here are the magic words. The self-assessment questionnaires that you want to look for when you are reducing scope are A and P2PE [2]:

- SAQ-A allows your organization to reduce your questions down to 22 for web transactions simply by never seeing a credit card number or having it pass through your website.
- SAQ-P2PE is a newer level of self-assessment questionnaire that allows merchants to reduce the scope of their questions by using certified point-to-point encryption solutions so that the merchant is never able to see credit card information. A number of payment processors are still in the dark regarding P2PE, and quite a few are still in the process of getting certified. We will talk more about this below.

Note that these questionnaires won't apply to you if you are doing custom, advanced solutions like major retailers, such as Home Depot or Target, but if you are in the midmarket or below, these questionnaires are gifts.

When it comes to determining the correct approach for your PCI-DSS assessment, ensuring your scope is accurate is of the utmost importance. If the scope of the assessment is not performed correctly/accurately, you could find yourself doing more work than is needed, or worse, not truly being compliant with your chosen SAQ.

Self-assessment options

The following are the various SAQ options allowed by the PCI Council:

SAQ Type

A (22 questions)

Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS-compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.

A-EP (191 questions)

E-commerce merchants who outsource all payment processing to PCI DSS-validated third parties and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*

B (41 questions)

Merchants using only imprint machines with no electronic cardholder data storage and/or standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

B-IP (82 questions)
Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

C-VT (79 questions)
Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS-validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*

C (160 questions)
Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*

P2PE (33 questions)
Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

D (329 questions)
For merchants: All merchants not included in descriptions for the above types.

D (370 questions)
For service providers: All service providers defined by a payment card brand as eligible to complete a self-assessment questionnaire.

As you can see, there are a lot of options, and it is crucial to select the correct one [1].

Effect of scope reduction

The net effect of scope reduction is dramatic. For example, if you are filling in a SAQ-P2PE with 33 total questions, most of these are around training, procedures, and documentation. In actuality, with a P2PE questionnaire you only have a limited number of pure security requirements, which are typically trivial for organizations with any level of information security management system. The biggest requirement to consider is the management and tracking of all P2PE hardware devices. A formal secure courier process, along with updating/maintaining a full inventory of each device, will be some of the most important things to implement for the P2PE. However, some P2PE vendors will provide assistance with these requirements, so when shopping around you should inquire if they do.

The same holds true for the SAQ-A. At only 22 questions, it is the simplest and easiest of all the questionnaires. The biggest thing to ensure here is that the outsourcing of all storage, processing, and payment of card data for your e-commerce is done through a PCI-validated third party. While independent validation should be done, when shopping around you should ask any vendor if their solution will qualify you for an SAQ-A.

One important note to mention about SAQs. If you have multiple payment channels (i.e., e-commerce, face-to-face in stores, etc.) you can complete an SAQ for each channel and not have to include them all in the same scope under one SAQ. As an example, if you have brick and mortar stores with P2PE devices only, and a website outsourced to a third party compliant with PCI, you can fill out and SAQ-A and SAQ-P2PE.

Selecting the right vendor

The first big issue facing companies is determining how their "PCI approved" vendors fit into these SAQs. It's very important to know that many companies that represent themselves as PCI-compliant vendors are not really telling you much about how exactly they are compliant. We've encountered multiple organizations saying they were PCI compliant, meaning compliant in the way they take credit cards, as a merchant, and that had absolutely nothing to do with being compliant as a service provider and helping you, as an organization, meet the PCI guidelines.

Scoping works both ways

Remember, since PCI allows you to scope, the scope of any implementation is critically important. We have seen companies hire a QSA to come in and perform an assessment, get their PCI-DSS report on compliance (RoC) and attestation of compliance (AoC), which certifies them as PCI compliant as a service provider and not just a merchant, as discussed in the previous paragraph. While it might seem on the surface that you as the customer have nothing to worry about, it is not that simple. There are two critical things to consider when assessing a PCI vendor/service provider: what's the scope of the PCI certification and who is responsible for what.

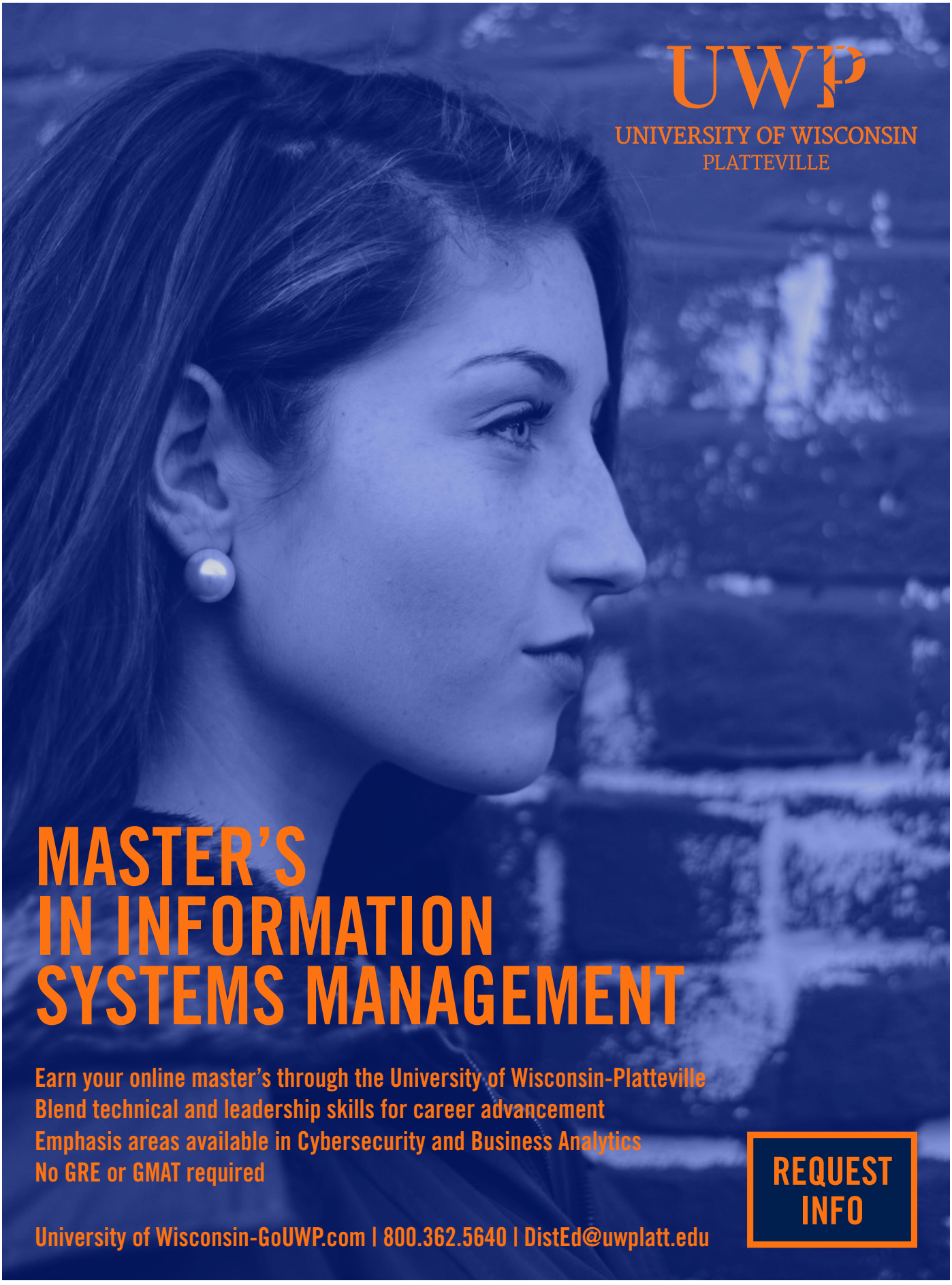
Responsibility matrix

As an example, let's say Acme Inc. has a managed intrusion detection service (IDS) that will potentially process packets that could contain encrypted cardholder data. Acme gets validated for PCI compliance. They can now say they are PCI compliant, except the scope of that assessment didn't cover the managed IDS system and its setup/compliance with PCI standards. You now use Acme Inc's IDS device, which is supposed to be PCI compliant and presume that your IDS responsibilities are now under the scope of Acme Inc's PCI responsibility. This is where the service provider *responsibility matrix* comes into play—essentially a document that should be provided by any PCI vendor that outlines question by question, control by control, what the vendor is claiming is your responsibility, what is theirs, and what is shared.

Vendor selection criteria

It's important that you be aware of the critical PCI-compliance elements to find out about your vendors. Please note that:

- The vendor you choose makes a difference. For example, one company chose a PCI-compliant vendor that could


UWP
UNIVERSITY OF WISCONSIN
PLATTEVILLE
MASTER'S
IN INFORMATION
SYSTEMS MANAGEMENT
Earn your online master's through the University of Wisconsin-Platteville
Blend technical and leadership skills for career advancement
Emphasis areas available in Cybersecurity and Business Analytics
No GRE or GMAT required
REQUEST
INFO
University of Wisconsin-GoUWP.com | 800.362.5640 | DistEd@uwplatt.edu

not provide a solution to meet the lower level SAQ-A questionnaire (22 questions). Instead the company would have needed to fill out a SAQ-A-EP (191 questions) and got a much longer, more stringent list of questions to answer and to which they were required to be compliant.

- Another company did not consider PCI compliance with regard to voice over IP phone systems. They now face a SAQ-D because their provider was not PCI certified. As a result, this organization had to fill out the most onerous of the self-assessment questionnaires to achieve compliance. We address this in greater detail in our case study section, below.

Case studies

Let's take a look at this from two different angles: taking credit cards in person or over the phone versus taking credit cards over the web. Keep in mind, that depending on the methodology you use, you can have to answer up to 329 questions. The goal is to significantly reduce this number *and* your risk exposure.

P2PE

In order to make it easier on merchants, in 2012 the PCI Council released the P2PE standard, which stands for point-to-point encryption [3]. When we work with companies to identify appropriate P2PE devices, we are often met with confusion on the part of payment processors because P2PE is seemingly not yet well understood. Interestingly enough, it is really very simple. If you acquire a P2PE device from a payment processor who is P2PE certified, you only have to fill out thirty-three (33) relatively easy questions to be compliant. And the process for taking credit cards is easy. You can dip the card if you have it physically present, or depending on the device, type the card number into the device. How hard is it to get it? You just have to ask the right vendor.

We've also found that from a cost perspective, these devices cost approximately the same as legacy systems. Interestingly, some companies have saved money by moving to a new provider. These savings come in many forms, and an especially big one is the reduction of in-scope systems that have to be included in the scope of an assessment each year. You can also save an enormous amount of time because when each year's PCI assessment rolls around, the amount of work, including evidence and screenshots, is greatly reduced.

>>Sidenote: Voice over IP: Plague or panacea

Of course, it wouldn't be a story without some drama. Here's the interesting potential caveat and a happy ending. In November 2018, the PCI Council distributed new guidance regarding usage of voice over IP (VOIP) to transit conversations that contain cardholder data [4]. The primary issue is that leveraging a voice over IP telephone system almost automatically gets you the full 329 questions of the SAQ-D because of the potential for compromising the data riding over a phone system. The good news is if your VOIP provider is PCI compliant, that's no longer a concern for you, and you can use the P2PE questionnaire with a limited scope. **Moral of this story:** be sure that nothing in your ecosystem ruins your ability to use a less onerous SAQ.

Note that the VoIP situation is complicated by having a call center, and that additional consideration needs to be applied should you record your calls. Dual-tone multi-frequency (DTMF) and automated speech recognition (ASR) are other options to keep cardholder data out of your VOIP scope. DTMF and ASR allow for routing credit card collection to a qualified and certified third-party provider, keeping that dangerous cardholder data off your network.

Web answers

Now, let's talk about the web. When you are designing a website and have to interface with a payment processor, you have a multitude of options. The PCI DSS is concerned about what access you might have to any credit card information when processing a credit card transaction. So, using an SAQ-A, the DSS gives you a couple of options by which you can bypass the maximum 329 questions of a D or the 191 questions of an A-EP (an option for some web implementations) by simply choosing an appropriate methodology and a vendor that supports it to lower your scope and get your number of questions down to the 22 relatively easy questions of an SAQ-A.

In the case of an SAQ-A, you either have to request the credit card via an i-frame (a way to embed access to another webpage in your webpage) or redirect to a website or code that is managed by your payment processor. And achieving this level of compliance is even easier than the P2PE model. You don't need to buy anything; you just need to make sure that the payment processor has a reasonable method by which you

Security, and Business, Metrics

Continued from page 7

health and safety needs to look at the environment and processes in order to issue orders to ensure that businesses and industries may continue to operate safely.

About the Author

Robert Slade has written a number of these columns, and the number of words in each is remarkably similar. His book on cybersecurity lessons that CoVID-19 is teaching us should be out soon, and he hopes a number of you will buy it. More metrics than anyone would want to know about him, and a number of links to bits from the book, are available at https://twitter.com/rslade. A number of people have tried to get him to take bio writing seriously; you can try too, at rslade@gmail.com.

can request a credit card number from your customer—that will get you an SAQ-A questionnaire.

Where to start?

You may want to work with an appropriate PCI expert to understand all the nuances and differences. For even a medium-size business, the difference in cost can be considerable for just the remediation alone. And, remember, the costs are not just what it takes to implement but also to *maintain* the system. Furthermore, even if you don't have direct access to cardholder data, you can still maintain your effective business workflow through your provider's software, including recurring payments.

As we all well know, IT vendors hold the keys to your kingdom. Depending on the nature of IT services you are purchasing, your risk can vary widely. For example, if you are using a vendor to do IT support, they likely have full administrative access to your system. That means they need to comply with all the laws, regulations, and contractual obligations that you have in place. Software vendors create software that you depend on, and it is virtually impossible to see what's going on under the hood. The situation is exacerbated if your software is hosted in a cloud solution, as that cloud provider typically has 100 percent access to your data all of the time. Additionally, you cannot forget about your phone system, which carries a significant amount of confidential information. The way a phone system is managed, from the handoff of a call from the traditional phone system to your VOIP phone on your desk, is critical to maintaining appropriate security.

Once you have researched a few vendors for your needs, there are some preliminary questions you should ask before proceeding:

- Are you PCI compliant? If so, what is your compliance date?
- What is the scope of your PCI compliance?
- Can you provide your attestation of compliance (AoC) for our review?
- Do you have a service provider responsibility matrix you provide to customers, outlining what responsibilities you cover, what we (the customer) need to cover, and what responsibilities are to be shared?
- If the merchant is a P2PE provider, have the device and software been specifically assessed against the PCI P2PE standard, and is it listed on the PCI website?

Conclusion

Vendor risk management is essential to appropriate information security hygiene. However, this goes to a completely different level when PCI is in the mix. If you process credit card transactions as part of your business, PCI compliance is a critical part of staying out of trouble both from the perspective of being able to take payments via credit card and from the possibility of significant fines and penalties should you have a breach or be audited.

In summary, the PCI Council gives you a number of excellent options for reducing your PCI scope and transferring responsibility to PCI compliant providers. By understanding your options, you can reduce cost and risk. Finally, always remember that YOU are responsible for maintaining the compliance of whatever the vendor does not explicitly claim responsibility for in writing. It is important to remember that one of the biggest reasons to use a vendor to process your credit cards is to outsource responsibility; if you are not getting that transfer of responsibility with your contract, you are not getting the most for your investment.

References

1. Mateaki, George. "PCI Standards: Which PCI SAQ Is Right for My Business?" Security Metrics – https://www.securitymetrics.com/blog/pci-standards-which-pci-saq-right-my-business#:~:text=Each%20SAQ%20includes%20a%20list,Requirements%20of%20PCI%20DSS%20Compliance%3F – an excellent blog post for a breakdown of SAQ requirements.
2. PCI SSC, "Completing Self Assessment," PCI Security Standards Council –https://www.pcisecuritystandards.org/pci_security/completing_self_assessment – for learning more about completing self-assessments.
3. PCI SSC, "P2PE Program," PCI Security Standards Council –https://www.pcisecuritystandards.org/pdfs/120627-P2PE-Program-Guide_SAQ_Update.pdf – P2PE announcement.
4. PCI SSC, "Protecting Telephone-Based Payment Card Data," PCI Security Standards Council – https://www.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf – information on configuring cardholder data transit over voice over IP.
5. PCI SSC, "SAQ Instructions," PCI Security Standards Council –https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2_1.pdf – page 3.
6. PCI SSC, "Why Security Matters," PCI Security Standards Council –https://www.pcisecuritystandards.org/pci_security/why_security_matters – an excellent discussion of the risks and impacts of a PCI-related breach.

About the Authors

R. Scott Pierangelo, MSCS, QSA, CISSP, CISA, CISM, CRISC, CGEIT, PMP, CDPSE, PCIP, is a founding partner of Silent Storm Security and has been conducting auditing assessments for over twelve years. He may be reached at spierangelo@silentstormsecurity.com.

David Lam, CISSP, CPP, is partner and CISO at Miller Kaplan. He has 33 years of IT experience in positions of increasing responsibility, 29 of which include information security. He may be reached at dlam@millerkaplan.com.