Strong and Healthy: PCI Security at Fairview Health Services

FAIRVIEW

Like other healthcare organizations, Fairview is also a merchant. As such, it is just as subject as any other merchant to the requirements of the Payment Card Industry (PCI) Data Security Standard for safeguarding cardholder data.

Recently, the organization began to grapple with questions, such as:

- What are our obligations under this standard?
- Who in the organization owns the effort to gain compliance? Which groups need to be involved?
- What payment applications and services are we currently using? Where is the cardholder data being stored and transmitted?
- What are the gaps between current practices and the requirements of the standard?
- How can Fairview reduce the time and cost involved in compliance efforts while still using security best practices?

Glen Allen, Fairview's Director of Information Security, was aware of the PCI Standard. "It's a good standard," he said, "because it is quite prescriptive, unlike, say, HIPAA, which is more general: do a risk analysis and go forth and do good security. It's a lot easier to get the necessary buy-in and sell PCI actions to senior management because the standard spells out what is required. PCI is also consistent with security best practices, so there is really no reason not to do it."

Because the PCI standard has some financial consequences for non-compliance, Glen worked with David Leach, Fairview's Assistant Treasurer. They determined that the PCI effort would be owned by David's department. Coincidentally, around this time Fairview's bank, Wells Fargo, put on a two-day seminar on PCI, and both executives attended.

About Fairview Health Services

Fairview Health Services, based in Minneapolis, is a not-for-profit, integrated healthcare network serving the Twin Cities, as well as communities in outstate Minnesota and the Upper Midwest. A nationally recognized leader in clinical excellence and innovation, Fairview is the fourth-largest healthcare services organization in Minnesota, as well as several Fairview hospitals and Fairview Behavioral Services. Revenues in 2008 were $2.8 billion. For more information, visit fairview.org.

Industry
Healthcare

Headquarters
Minneapolis, MN

Reach
Upper Midwest

The Role of a Security Consultant in the SAQ

One of the first steps in gaining PCI compliance is to complete the Self-Assessment Questionnaire (SAQ). The name is a bit of a misnomer, because some of the 228 questions require interpretation and expert advice. Glen Allen recommended NetSPI for this job: "We already had a relationship with NetSPI, having used them for a security assessment, and were just starting to use them in an internal audit capacity. As a security manager, I was happy with the work they had done in the security assessments and felt they would be easy to work with on PCI."

As David Leach explained, "We were struggling to fill out the SAQ. The biggest challenge was figuring out all the places where credit card data resided. Different departments and facilities had different POS systems, applications, and merchant relationships."

Gap Analysis

Paul Johnson, NetSPI's Director of Consulting, noted that, "To start the process, we did a gap analysis. First, we interviewed all the different business groups within Fairview handling credit card transactions. There were more than was generally realized. Besides registration and billing functions, there were clinics, in-patient facilities, home care, pharmacies, cafeterias, gift shops – even parking ramps. NetSPI looked at the POS systems used in each location and the payment applications, as well as the physical handling of hard copy records with credit data. We documented any gaps between current practice and PCI requirements."

Then NetSPI went to the IT people at Fairview, to understand more technical information on topics like where and how credit card data was stored, which payment applications were used, and over which network segments the data moved. Understanding the payment acceptance channels and the data flow was necessary to determine the scope.

Armed with that information, NetSPI was able to help Fairview accurately complete the SAQ. As a certified QSA that has been through many of these SAQs, NetSPI consultants were able to interpret the intent of questions and explain what the PCI Council is looking for on particular questions. For example, is there some leeway on a particular item? What mitigating factors come into play? Is there a grace period for implementing required changes?

As David Leach noted, "It's really helpful to have someone who has gone through the SAQ process a number of times to advise us on what would pass muster. We don't know the standard well enough to know, for example, that a particular mitigating factor will not last. In addition, these are relatively new and changing standards. We were in the

It's a lot easier to get the necessary buy-in and sell PCI actions to senior management because the standard spells out what is required. PCI is also consistent with security best practices, so there is really no reason not to do it.

Glen Allen

Director of Information Security at Fairview

middle of working through Version 1.0 when Version 1.1 was released. And 1.2 is now the current standard."

Implementing Changes After the SAQ: The PCI Island

With NetSPI's help, completing the SAQ didn't take very long. Then came the planning of what needed to be done. The basic strategy was to set up a "PCI island," or in other words, to restrict the number of network elements that transmit, process, or store credit card data and thereby reduce the scope and complexity of achieving compliance.

David Leach explained, "There are a lot of technical pieces involved in setting up a PCI island. And there are impacts on various business units. So, we had to figure out who needed to be in the room to work on this project." Specifically they needed to understand who would be responsible for each of these three areas:

1. **Technology Piece.** This includes the servers, firewalls, intrusion detection systems, applications, etc. David Leach noted, "I know there are things called servers and firewalls. But I don't need or want to know more about them than that. This is where the IT people are needed."
2. **Banking Piece.** Fairview needs to have merchant accounts with banks like Wells Fargo and therefore needs to be in compliance with the PCI standard. This piece is owned by the Treasury Department at Fairview.
3. **Business Owner Piece.** The people running the various departments that use credit cards need to understand the implications of PCI for their business processes. For example, they need to know what they can do if there is no compliant version of an application that they are currently using.

David Leach worked with all three groups, to design the technical elements of the PCI island, to find out about compliant applications, and to understand the business requirements and help with any necessary process changes. He explained, "Now we monitor the things on the island and the things that connect to it, because we have reduced the scope of our compliance effort. So, for example, our pharmacy app needed to be on the PCI island, but our general ledger app did not."

There is another advantage to the PCI island. The PCI standard imposes some security burdens on users that are not always welcome. For example, some Fairview employees complained about automatic logouts after 10 minutes. Ditto for changing passwords frequently. Restricting the scope avoids having to impose those security measures on many users. As David Leach noted, "We are taking credit card data out of some of our own apps and just using vendor-supported compliant apps, to relieve the burden on users."

> "It's really helpful to have someone who has gone through the SAQ process a number of times to advise us on what would pass muster.
>
> **David Leach**
>
> *Assistant Treasurer at Fairview*

Beyond the SAQ: Internal Audit and External Scans

Because Fairview does not have its own auditors with a wide breadth of IT experience, the Internal Audit group has decided to partner with an outside security-assessment firm, in this case NetSPI, and co-source ongoing audits.

The division of labor works like this: NetSPI does the security assessment on a given technology, and then Glen Allen, Internal Audit, and NetSPI work to turn those results into audit findings. As Glen Allen explained, "An assessment is going to come back and say 'This control is not in place, and we consider that a high-level vulnerability.' That is not an assessment of risk, not an actionable item. Internal Audit turns that into a risk statement, spelling out the likelihood that this vulnerability will be exploited and the potential consequences."

For example, one of the audit projects involved wireless applications. NetSPI looked at the wireless access points (APs), what encryption was being used, and whether Fairview was configuring and managing the wireless devices with security best practices. These wireless devices are used throughout Fairview facilities for many purposes, from medical applications like matching blood samples with patients, to standard business applications like checking bar codes on incoming supplies.

NetSPI, a certified ASV, is also conducting quarterly external scans of the Fairview network, as part of ongoing compliance work. The early scans covered a large scope. David Leach noted, "We learned some useful things from those scans, e.g., about generic logins being used or web sites that were not properly set up. But now that we have reduced the PCI scope, the scans cover a much smaller scope and take fare less time." Glen Allen added, "We realized that it isn't necessary to store cardholder data 'just in case.' If we don't need it, we don't store it. That helps significantly in reducing the scope."

Fairview expects to have NetSPI continue to validate compliance with regular PCI audits. As the old adage says, security is a process, not a product.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.

Website
www.NetSPI.com

Email
Info@NetSPI.com

Phone
612.465.8880