netSPI Case Study

RISK COMPLIANCE SECURITY

HealthEast

NetSPI Helps HealthEast Counter Security Threats from Inside and Outside

Healthcare organizations today face a unique set of security challenges. For one thing, HIPAA, the Health Insurance Portability and Accountability Act, lays out principles and goals for ensuring the privacy of patient-identifiable data. Similarly, PCI, or the Payment Card Industry, has a very detailed Data Security Standard for safeguarding personal information in credit card transactions, which are now part of hospital and pharmacy operations everywhere.

In addition, healthcare organizations face a cultural hurdle. Historically, they did not put the same emphasis on data security as, say, financial institutions, nor did they have the same budgets or staff dedicated to security as banks or brokerages. The institutional mindset was focused not on maintaining security but rather on providing care. As a result, when new technology was introduced or expanded from a department to a broader network, the emphasis was usually on the new functionalities, not on new potential vulnerabilities.

All these issues are familiar to HealthEast, the largest, locally owned healthcare organization in the Twin Cities' East Metro area. With 6,700 employees and 1,400 physicians on staff, HealthEast includes Bethesda Hospital, St. John's Hospital, St. Joseph's Hospital, and Woodwinds Health Campus, as well as outpatient services, clinics, pharmacies, home care services, and transportation services.

Delivering on Security and the HealthEast Mission

When it comes to security, HealthEast is determined to do the right thing, but not at the expense of the organizational mission. As Ron Strachan, VP and Chief Information Officer, put it, "We strive for a balance, making sure the steps we take for security are not so restrictive as to prevent our people from doing their jobs." The organization's culture needs to be taken into account. As Strachan noted, "Some employees may not be enthusiastic about being asked to do an additional step or two. When we explain that it's for security, they may say, 'I'm not going to do anything wrong. Why should that affect me?' They don't think about the big security picture, and they're not being paid to do so. That's our job."

CASE STUDY AT A GLANCE

Client

HealthEast is the largest locally owned healthcare organization in the Twin Cities' East Metro area. With 6,700 employees and 1,400 physicians on staff, HealthEast includes Bethesda Hospital, St. John's Hospital, St. Joseph's Hospital, and Woodwinds Health Campus, as well as outpatient services, clinics, pharmacies, home care services, and transportation services.

Challenge

Understand internal and external threats as well as vulnerabilities in applications, systems, and technologies.

Solution

NetSPI has undertaken a range of projects for HealthEast, including risk analysis and a variety of assessments: external, internal, physical security, PCI compliance readiness, and application security.

Results

"Their processes are very structured…Everything happens the same way every time. There are no surprises. And their reports are phenomenal compared with some of the others we have seen. They are way above any one else."

Facing a Variety of Vulnerabilities

Today, HealthEast faces three kinds of vulnerabilities. First, there are threats from the outside. "Our networks and our Internet sites are available to some extent to the public. We insulate our networks, but of necessity we have to allow some access," Strachan said.

Second, HealthEast faces internal threats—employees doing bad or thoughtless things, or both. "For instance, "Strachan said, "an employee with a laptop containing important patient data might leave it in his car in the driveway. Surprise! It gets stolen. We can't prevent the act from happening. But we can prevent the asset from being misused by requiring strong authentication to use the laptop or encryption to protect the data, or both." Third, there are vulnerabilities in applications, systems, and technologies that HealthEast acquires and uses. "Their products are not intended to be unsafe, but many vendors do not think about security first," said Bonnie Anderson, System Director of Information Security for HealthEast. "There is often a gap between what we expect and what they deliver. So we have to mitigate those gaps."

In general, said Kristi Reese, Senior Security Analyst, Information Technology, "We assume people both inside and outside the organization will sometimes do things that run counter to our policies. We have to ask: what's the worst thing that can happen? Then we put measures in place to mitigate those possible consequences."

Mitigating Risk

As part of those efforts, HealthEast retained NetSPI to help identify and mitigate security risks in all three areas. As Reese noted, "One big way NetSPI helped us was in validation. We can implement security policies and measures, but one change can inadvertently create a huge hole, and it's hard to know that when you are inside. So having NetSPI testing from the outside was huge for us." NetSPI has undertaken a range of projects for HealthEast, including risk analysis and a variety of assessments: external, internal, physical security, PCI compliance readiness, and applications.

Application Dangers

With regard to the last area, assessments are especially important for new web-based applications. For example, there was a radiology imaging application with great promise. It would store X-rays and scanned images digitally, replacing film and eliminating the problem of lost or misplaced slides. It would also enable doctors to view the images from anywhere via the Internet. "We had a lot of problems with residual data with this application," Reese noted. "Say a doctor was viewing radiology images in a place with open Internet access and briefly left his laptop unattended. Someone could walk up to the laptop and, using a simple software program, capture patient-identifiable data that could be used for malicious purposes. NetSPI has been invaluable to us in the investigation of that application," Reese said.

Anderson concurred: "I really appreciate the fact that NetSPI goes beyond just saying that there's a hole in some application. They actually show how the vulnerability can be

> ***"Their processes are very structured. Everything happens the same way every time. There are no surprises. And their reports are phenomenal compared with some of the others we have seen. They are way above any one else."***
>
> Kristi Reese,
> Senior Security Analyst,
> Information Technology,
> HealthEast

netSPI
RISK COMPLIANCE SECURITY

exploited. They say, 'This is what we were able to do.' They will actually have a screen shot that says 'NetSPI was here,' demonstrating the possible exploitation. Other firms will just say a vulnerability exists and could possibly be exploited. NetSPI proves it. And they have great people that they send out here—very competent and helpful."

Structured Processes

HealthEast is impressed with the way NetSPI does its job. "Their processes are very structured," Reese said. "Everything happens the same way every time. There are no surprises. And their reports are phenomenal compared with some of the others we have seen. They are way above any one else."

Currently, NetSPI is helping HealthEast comply with the PCI standard for securing credit card information. Developed by card brands like MasterCard and Visa, the PCI Data Security Standard is very detailed compared with HIPAA. The standard groups users into tiers according to how many transactions they handle in a year. If a merchant has a security breach and is not PCI-compliant, then the merchant (including, say, a pharmacy in a hospital) is on the hook for any losses incurred. On the other hand, if you are PCI-compliant, then your processing fees will be lower. NetSPI recommended increasing external assessments for PCI compliance, from two to four a year, in order to help ensure data privacy.

Continuing Assessments

Beyond that, HealthEast expects to continue using NetSPI for a variety of projects designed to ensure compliance with HIPAA and PCI standards. After all, maintaining security in a modern healthcare organization is a continuous process with constantly changing threats and vulnerabilities.

800 Washington Avenue North, Suite 670, Minneapolis, Minnesota 55401
www.netspi.com 612.465.8880 Telephone 888.270.0317 Toll free 612.455.6988 Facsimile