

<http://www.itcinstitute.com/display.aspx?id=4566>

Best Practices

Case Study: A Healthy Sense of Security

While reacting to changes in the market, a health care services company has proactively tightened down security beyond HIPAA and aims for certification on the relatively tough ISO 27001 standard.

By Linda L. Briggs

November, 2007

It's all too common for companies to wait until there's been a security breach to instigate stricter data controls. American Imaging Management (AIM), a nationwide medical services company based in Illinois, decided last year to take a proactive stance instead. Reacting to the greatly increased use of technology in managing health care information, as well as a customer request, the company moved quickly to instigate a rigorous ISO 27001-based security assessment in 2006. The company is now confident of formal registration as an ISO 27001-compliant firm in early 2008, a relatively rare achievement for a US company.

AIM helps health plan providers manage their health plans, including outpatient diagnostic image management services, utilization management, provider network development, and claims adjudication and provider payment. In offering those services, AIM exchanges patient information with a range of health care entities, including health plans, physicians, and imaging facilities. The 500-employee firm has just 24 clients nationwide, but that number is deceptive: AIM's clients provide health care plans to some 20 million people.

According to Kristine Tomzik, who is AIM's VP of compliance and chief compliance officer, as well as a registered nurse and Certified Professional in Healthcare Quality, AIM decided to pursue ISO 27001 certification last year as "a proactive strategy to better position us in the marketplace." Ongoing changes in the electronic environment, especially regarding the electronic exchange of health information, were making security more and more a top priority for customers and for AIM itself. AIM chose the rigors of an ISO 27001 assessment because, Tomzik says, "to the best of our knowledge, it has the most stringent regulatory requirements around the protection of electronic information." Expediting the decision, one of AIM's clients requested that the company become ISO-certified.

That request may become increasingly common in health care, as more and more states move to stiffen federally mandated HIPAA security requirements through legislation. The new state laws often echo portions of the ISO 27000 standard without referencing it directly. Some new state laws regarding patient information management follow ISO's lead, for example, in taking privacy standards that HIPAA designates as optional (or "addressable," in the language of HIPAA) and making them required. ISO is also much more specific: While HIPAA specifies that patient health information must be protected, ISO 27001 goes further by specifying the actual controls a company should put in place to protect that information.

A specification for an information security management system, ISO 27001 is a key component in the developing 27000 family of standards, all of which pertain to information security. 27001 is the primary document and is intended to be used alongside other ISO standards that will contain additional details; just three documents have been published so far in the 27000 family.

Choosing an Outside Consultant

Lacking the time and expertise in its 60-person internal IT department for an ISO certification assessment, AIM decided to work with an outside security firm and eventually selected Halock Security Labs, an Illinois- based information security consultancy.

In mid-2006, Halock began an initial gap assessment with AIM; things moved quickly from there. Within 45 days, the assessment was completed and the company, together with Halock, then prioritized which security issues to address immediately, and which would take more time. Through the following months, a Halock representative worked as a member of AIM's standing security governance committee, a team of four to six people that included representatives from IT, senior management, compliance, and various internal departments.

According to Inna Berkovich, senior VP and CIO for AIM, the gap assessment looked at security policies AIM already had in place, including policies and procedures, password controls, firewalls, and AIM's internal audit process for information access. Halock also worked with AIM to examine areas such as HR policies and procedures regarding employee training. The assessment looked at security enforcement measures as well: Whether appropriate disciplinary rules were in place, and whether AIM's structure provided appropriate oversight of the IT department.

At around the same time, AIM also used a security expert from an outside firm unrelated to Halock that specializes in vulnerability assessments to attempt to "hack" into its systems. The key security issue that emerged from that, which AIM quickly repaired: The ability of an outsider to access SQL code and modify its content.

Starting from a Strong Base

One reason the assessment and remediation proceeded relatively quickly is that AIM already had solid security controls in place. In that sense AIM was unusual, according to Neil Witek, part of Halock's governance and strategy team and AIM's key contact. What AIM lacked, he says, was a consistency in overall management of those controls. "Since ISO is about management, not just good controls," he explains, that issue became the focus of AIM's remediation efforts.

"They had their act together," he says of his initial assessment of AIM in mid-2006. "They had a release schedule, a mature change management process, a mature network architecture and firewall. It just wasn't consistently managed." Also missing was a plan for continual improvement, something ISO emphasizes as part of its focus on ongoing monitoring and process improvement.

After the gap analysis identified potential problem areas, Halock worked with AIM to produce a remediation plan. That's where ISO 27001 came in handy, Tomzik says, since the standard has a useful "walk-the-talk component. You not only look at policies and procedures, but take it a step further," by checking to make sure they actually work.

AIM now conducts quarterly reviews of its security policies, per ISO policy, and has designated a security officer as well, also per ISO. AIM also conducts full vulnerability tests of its software system each quarter. That includes having an outside security expert attempt to breach the system, using the latest tools and techniques. Based on that, AIM continues to tighten any exposure it finds, although the list has dwindled rapidly. "We had issues to address the first time around," Berkovich says. "The next time, we were pleasantly surprised... They found a few high-priority items." Now, the quarterly reviews might turn up one or two issues of medium priority.

Security a Growing Priority

As the medical industry focuses more on security, it's becoming more common to see Requests for Proposals containing security stipulations that could have come directly from ISO 27001, according to Paul Danao, AIM's VP of business development. He says that in a recent RFP, although ISO wasn't specifically mentioned, "there were almost as many questions on security and the handling of information as there were on the actual program and program design."

He attributes that trend to health plans becoming much more aware of the importance of information security, partly spurred by HIPAA. But ISO goes well beyond what HIPAA requires at a federal level, and in doing so, he sees it raising the bar on vendor expectations. "A lot of what [RFPs] ask about now," Danao says, "are areas covered under ISO."

Calculating the Returns

For now, AIM's pending ISO registration will pay off by giving clients a sense of confidence in how the company handles health care records. Eventually, Hallock's Wilek speculates, the ISO registration may allow AIM to bypass the numerous annual security audits it now undertakes to satisfy individual clients. Instead, AIM will be able to "just staple [its] security registration to the application."

In terms of a direct return on investment, however, Wilek says he didn't present the ISO process that way, nor did the company regard it in that light. "AIM didn't view it as an investment, but rather as risk management," Wilek says, "just like someone buying insurance."

Berkovich, Tomzik and Danao all point out that although calculating a direct return on investment is difficult, the costs of a security failure could be huge for AIM -- or for any other company in AIM's position. That's partly because regulations around the protection of health care information are tightening. California, for example, has passed legislation that will go into effect in January 2008 mandating that consumers must be notified of a health care data breach, just as must be done now with financial data.

For AIM, which often works with plan providers who cover a million members or more, that could make a security mop-up hugely expensive. "The costs associated with the state-mandated disclosure go beyond the 42-cent stamp on the letter, and the time to generate the letter," Berkovich says. And there's also this, she points out: "If you breach client's data, you may lose a client. And there's your ROI right there."

"Looking at where the [health care] industry is going, " Danao says, "we think having the security in place will translate to a financial return just based on our ability to win and retain clients... We will be able to demonstrate to clients that we take security seriously, and that we have an effective program in place."

Linda Briggs is the founding editor of Microsoft Certified Professional Magazine and a former senior editorial director at 101communications. Based in San Diego, she writes about technology in corporate, education, and government markets. You can contact her about this and other articles at lbriggs@lindabriggs.com.