Eat the Frog: Time for a Privacy Risk Analysis

Let's be honest—performing a security risk analysis is the worst

By Mary M. A. Potter, CISA, CRISC

As an IT auditor or audit manager, we are often tasked with performing the security risk analysis for the system we support. In order to be compliant with the HIPAA Privacy Rule, providers are required to perform reviews of the risks associated with their handling of protected health information (PHI).

The statute requires providers to review the protections around electronic PHI periodically. If your facility receives Meaningful Use incentives, you are required to perform this analysis annually. The results of the analysis are mainly centered on PHI but are applicable to all of the confidential information within your organization.

The risk analysis performed should be "an accurate and thorough assessment of the potential risks and vulnerability to the confidentiality, integrity and availability of electronic protected health information."

So what does this mean?

You have to look at each of the elements in the regulation and identify the good, the bad and the ugly. The analysis will include all of your policies as well as the physical and technical safeguards.

Honesty speaking—as a geek—technical safeguards are the best. We love to brag about the technology we have in place and use the risk analysis as an opportunity to moan about what the other guys have that we really want. Geeks see this process as a way to justify new toys. We know you do too, so just admit it.

Since we all hate sitting in a room reviewing policies for hours, what is the best way to evaluate the controls you have in place and identify the ones you do not? The process is resource-intensive, can be tedious and is clearly a political landmine.

A look at your options

There are three basic options in this process.

Option 1 – Don't do a risk analysis and pray you will not be audited

You might have excellent karma and might be able to get away with it, but I doubt it. The Office of Civil Rights has stated that this is one of the most significant areas of failure by covered entities.

Plenty of evidence shows that not having a periodic risk analysis will result in larger fines in the event of a breach. Just look at the fines for "willful neglect." If your organization is selected for an audit and does not have a reasonable risk analysis undertaken, your management will see this as a resume-generating event for all those involved in the decision to "wait on the analysis".

Option 2 – Perform the risk analysis in-house

The first question to consider is: Do we as an organization have a team that can adequately perform the audit? Do we have the skill set, the understanding of the requirements, the time and the validation tools within the organization? Keep in mind that the analysis should be objective, so using resources from other departments may not be an option.

Look at the pros and cons of keeping the review in-house.

Because you know your organization, you know who to call, where the policies are located and who owns them. This may make it easier to gather the information and require

There will be process or technology gaps, and if there are not, then you should question whether the risk analysis was performed adequately.

less time for the initial part of the review. Another possible pro is the cost. Although it is less expensive than hiring someone from the outside, your staff will be taken away from performing other activities, so it is not free.

Do not forget the cons. Internal audit expends a great deal of time building relationships with management at all levels. We provide consultation for their projects and help assess their departments. I would venture to say that we may have a friendly relationship with those audited. As auditors, we work to keep our reviews objective at all times, but we do lose some objectivity.

Because we may know the area well, or think we do, we may make assumptions about the effectiveness of the controls in place. In addition, because the full risk analysis may cross departmental boundaries, there will be friction, no matter how refined your diplomacy skills may be. If you have not performed a full scale review before, you may want to consider Option 3.

Option 3. Outsourcing

Outsourcing means that you will have the fun of meeting lots of consultants. They will try to take you to lunch and will give you lots of glossy brochures that you can use to line your wastebasket. Most of them will be very well dressed and may have absolutely no technical understanding whatsoever.

The pros of outsourcing are the limitation of internal bias and limited disruption of day-to-day operations. You may also be able to stretch the engagement to the development of objective action plans. If you choose this path, consider balancing periodic external analysis with annual internal reviews.

Carefully consider your strategy for selecting a consultant. Engage related stakeholders to consider the scope of the review and determine who the decision makers will be. Review potential consultants for their methodology, track record, cost structure, and whether they have other relationships to your organization that may limit their ability to provide an objective analysis.

When you have selected a consulting service that meets your needs, be sure to manage the relationship carefully. Be cautious not to allow the scope of the analysis to expand without consideration. If you are not watchful, a six-week risk analysis can become a one-year project with them moving into the office down the hall.

The auditor gets audited

Next comes the part where the tables turn. You are now answering the questions and gathering information. Assist the consultants with getting access to the right people within your organization.

Don't become the client we all hate. You know the one I mean—the one who carefully parses every question and only answers the very confined, literal interpretation of the question. They respond to what you asked but not what you really need to know.

If your facility receives Meaningful Use incentives, you are required to perform an analysis of electronic PHI protections.

This type of external risk analysis is no time to hide out-of-date policies, or show them the up-to-date server "at random" when you know it is the only one in the room with the security updates deployed. Take advantage of having the consultants in house to get a clear view of process or technology gaps. There will be gaps, and if there are not, then you should question whether the risk analysis was performed adequately.

A walk through ulcer gulch

Regardless of the path selected, you will end up with a completed risk analysis. At this point, you have gone through the process of files being poked at, servers being

prodded, and your network being laid bare for the entire world to see. You have negotiated the wording of the findings, argued that policies are comprehensive, and wordsmithed the final report to prevent your management team from stroking out. The easiest part of the process is now behind you.

You now have a list of various things that will give you heartburn. So pull out the Tums and start considering how to find the time, the people and the financial resources to correct each of the items on the list. Lack of time, staff, or money no longer matters. You must not only create a realistic action plan—you must actually implement it.

Step 1 – Read the analysis report.

Step 2 – Get a paper bag and breathe slowly until your hyperventilation is under control.

Step 3 – Read the analysis again, and start looking for ways to break the tasks up so they are in manageable pieces. Take into consideration that not all of the pieces may belong to your team or even your organization. If the findings are truly significant and unmanageable, consider employing outside resources to determine and implement a resolution.

Step 4 – For each of the items requiring an action, determine if the item requires new technologies to be deployed, additional resources for monitoring, or if the risk can be mitigated through policy and education.

Step 5 – Consider additional costs and timelines to deploy. Try not to be too specific in your commitments until you can determine if there are hidden deployment challenges. Remember to bring in key stakeholders to assist.

Conclusion

The time-management advice to "eat the frog"—to face the most difficult task first—applies throughout this process. Remember that you will survive to analyze another day. Although "frog-eating" can be distasteful, the risk analysis is an important part of your compliance with HIPAA and Meaningful Use. More importantly, it is a way to assure the right controls are in place to protect confidential patient, employee and business information. **NP**

Mary M. A. Potter, CISA, CRISC, is the Chief Information Security Officer for Carilion Clinic in Roanoke, Va. She works closely with the internal audit and compliance professionals to teach them the "magic" of information security protections. She has over 20 years' experience in IT. She welcomes communicating with those who seek to learn the language and ways of IT. Mary can be reached at MMPotter@cairlionclinic.org or (540) 224-5759.

Some Advice on Security and Disaster Recovery – continued from page 32

PCI and a host of other regulations—can provide holistic appraisal of your organization's risk, greater efficiency and a method for cooperatively managing your security controls and compliance.

Every organization is different and therefore will have a unique set of risks. It is important to take a holistic look at your organization's risk through thoughtful risk assessment, identification, analysis and mitigation.

All-inclusive frameworks tend to be broad enough so that an organization can adapt the concepts to their environment. It is important to remember there will still be a necessary investment of your time internally to make it work for you.

Q What about disaster recovery preparedness as it relates to social engineering?

A Your organization's disaster recovery plan should take into account the risk of a breach due to social engineering attacks. As a whole, IT administrators and internal audit departments have historically spent significant time focused on preventative measures. But data breaches are a matter of when, not if, and it is critical to shift some of your focus to the resiliency of your systems and data to ensure some level of business continuity in the event of a breach.

Your disaster recovery plan should also incorporate an incident response plan that details how your IT department should respond and proceed in the case of a breach. And, remember—disaster recovery plans should be periodically reviewed and tested. **NP**