The Anatomy of Risk

We all know that conducting a risk analysis is required for Meaningful Use attesting providers as well as to comply with HIPAA. Knowing that it is required is the easy part, understanding how to conduct a risk analysis, knowing where to start is a bit harder.

A risk analysis is a mathematical (stop cringing – it's a really simple formula):

Risk = (Threats X Vulnerabilities X Impact) – Controls

There are several variations of this formula; however, this is the simplest way to view risks. This formula will work in most organizations. Before you get too overwhelmed, let's explain what each of these variables mean as they relate to your assessment of risk in your organization.

If you view each term in relation to your home versus your technical environment, it is much easier to understand how each variable relates to risk. A **threat** is an external force – like an intruder or severe weather – that has the potential of causing harm to your environment. A **vulnerability** is a weakness – like windows/doors, or open Wi-Fi – that could allow a threat access to your environment if not properly managed. **Impact** is the cost – whether financial, operational, legal, or reputational – if the threat is able to exploit a vulnerability. **Controls** are the procedures and effort spent on the procedures to minimize the likelihood of a threat having the ability to exploit a vulnerability as well as controlling the impact to your environment.

There are many different methodologies for conducting a risk analysis, the majority of which are acceptable. There are, however, several important steps that must be included in your risk analysis.

1. **Scope the Assessment** – Identify where Protected Health Information (PHI) is created, received, maintained, processed or transmitted. Ensure to take into consideration remote workforce as well as portable devices and personal devices.
2. **Gather Information** – This is the step you will analyze the information in Step 1.
3. **Identify Realistic Threats** – Compile a threat statement or perform threat modeling (whichever is most reasonable for your organization). The listing of threat sources should include realistic and probable human and natural incidents that could have a negative impact on your organization's ability to protect PHI.
4. **Identify Potential Vulnerabilities** – Be sure to consider vulnerabilities to your physical and technical environments as well as your administrative processes. Consider areas where your PHI can be disclosed without proper authorization, improperly modified, or made unavailable when needed.
5. **Assess Current Security Controls** – Determine if the current implemented or planned security controls will minimize or eliminate risks to PHI.
6. **Determine the Likelihood and Impact of a Threat Exercising a Vulnerability** – This one can be difficult as it is can be subjective. An application and data criticality analysis can be helpful in completing this step. (Big words to mean determine the interoperability of your systems and what it would be mean if a system were to be unavailable). Be sure to consider the impact to your organization's legal, operational, reputational, and financial health if a threat were to exercise a vulnerability.
7. **Recommend Security Controls** – Determine what steps need to be implemented in order to further reduce the likelihood of a threat exercising a vulnerability. Knowing the risks is only the first step. Determining how the risks will be mitigated or managed in order to reduce their impact, is vital to the health of your organization.
8. **Document Results** – In healthcare, we understand that if it isn't documented, it didn't happen. This is also true of your risk analysis. This step is arguably the most important step. If you ever experience a breach or are chosen for an audit, this will be the first thing you are asked to produce.

Sarah Badahman
HIPAAtrek™
www.HIPAAtrek.com