DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

   By Marcelo Carvalho – ISSA member, Brasil Chapter
   This article discusses access control in the healthcare environment. Role-based access control capabilities and examples of dynamic requirements for controlling electronic health record systems in the context of healthcare professional use are described.

Articles

20. Cybersecurity Risk in Health Care
   By Barry S. Herrin – ISSA member, Metro Atlanta Chapter
   This article discusses the current state of healthcare data privacy and security, the legal issues requiring attention, risks of the growing use of remote and wearable technologies, and cybersecurity insurance.

25. Healthcare Security Ailments and Treatments the World Needs to Know
   By Jon Sternstein - ISSA Member, Raleigh Chapter
   This article provides insight into the immense data breach problem affecting the healthcare industry and closes with actionable solutions that all healthcare organizations should be accomplishing to minimize the risk of data breach.

32. Medical Data Sharing: Establishing Trust in Health Information Exchange
   By Barbara Filkins
   Interoperability is a critical healthcare industry initiative. Trust, however, is a major barrier to achieving seamless medical data exchange. This article describes what a trust framework is, along with the implementation challenges associated with trustworthy sharing of health-related data.

39. Leveraging a Control-Based Framework to Simplify the Risk Analysis Process
   By Bryan S. Cline – ISSA member, North Texas Chapter
   In this article, the author discusses HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.

Also in this Issue

3. From the President
   Hello, ISSA Members and Friends

5. Sabett’s Brief
   Healthcare and Infosec: Still a Work in Progress

6. Herding Cats
   Healthcare Is a Snowflake

7. Gray Hat
   Trusted Systems in Health

8. Open Forum
   Don’t Blame the Victims

   Minimizing Risk in an Ever-Increasing, Connected Health World

10. Security in the News

11. Letters

12. Association News

©2017 Information Systems Security Association, Inc. (ISSA)
The ISSA Journal (1949-0550) is published monthly by Information Systems Security Association
11130 Sunrise Valley Drive, Suite 350, Reston, Virginia 20191
703.234.4095 (Direct) • +1 703.437.4377 (National/International)
Leveraging a Control-Based Framework to Simplify the Risk Analysis Process

By Bryan S. Cline – ISSA member, North Texas Chapter

In this article, the author discusses HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.

Abstract

The risk analysis required by the HIPAA Security Rule is perhaps one of the most difficult for many healthcare entities to address, especially smaller ones like physician practices. Why? Most simply do not have the expertise and often lack the funding necessary to hire a professional services firm. However, there is another approach that is easy to adopt and readily available—a framework-based approach. In this article, the author discusses the HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.

Compliance with the Health Insurance Portability and Accountability Act [7] (HIPAA) Security Rule1 (the Rule) is arguably the principle driver for many organizations in the healthcare industry to implement the technical, physical, and administrative controls necessary to safeguard patient health information. However, the Rule’s standards and implementation specifications for these controls generally lack the specificity required for uniform implementation across the industry; nor are they comprehensive enough to ensure adequate protection of sensitive health systems and information in an ever-changing threat environment.

Fortunately, the Rule also requires healthcare organizations2 to conduct a risk analysis: “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information”3 … [to] “protect against any reasonably anticipated threats or hazards to the security or integrity of such information.”4 Such a risk analysis would help organizations determine the specific safeguards they should implement to protect patient health information, regardless of what may or may not be specified in the Rule.

Unfortunately, however, the risk analysis requirement has proven problematic for many healthcare organizations. The Office of Civil Rights (OCR) cited an incomplete or inaccurate risk analysis for fully two-thirds of the organizations evaluated against the first OCR audit protocol [15], conducted as part of a program mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act [8].

Risk analysis

To understand why the HIPAA risk analysis requirement is so difficult for these healthcare organizations, one only needs to look at a typical risk analysis process as depicted in figure 1, consistent with the Rule’s legislative language.

---

1 See 45 CFR Part 164
2 Covered entities and their business associates, as defined in 45 CFR § 164.102
3 See 45 CFR § 164.308(a)(1)
4 See 45 CFR § 164.306(a)(2)
A complete set of security controls must still be specified. HHS includes this control specification in the last step along with specific remediation plans based on the control gap analysis.

**Risk analysis in the risk management process**

The risk management process can be represented by a general four-step process model [2] as shown in figure 2, which includes identifying risks and information protection requirements, specifying controls, implementing and managing controls, and assessing and reporting on the controls. This first step is essentially the risk analysis process described earlier. But whether control specification occurs at the end of the risk analysis—as in the HHS model—or just after the risk analysis in the model presented here, control specification follows information classification, asset categorization, threat analysis, vulnerability analysis, and the calculation, ranking and treatment of risk (figure 3).

**Framework-based risk analysis**

The National Institute of Technology and Standards (NIST), while taking a similar approach to risk analysis as the HHS\(^5\) [12], specifies a slightly different risk management approach with their six-step model [13] depicted in figure 4.

\(^5\) The federal government considers the terms *risk analysis* and *risk assessment* synonymous.
Rather than perform the type of risk analysis first described, federal agencies categorize their information systems based on a more limited analysis focused on identifying “one of three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability)” [10]. Agencies then simply select a security control baseline appropriate for the categorization.

This is possible because major elements of the risk analysis have already been performed. For all intents and purposes, NIST conducted a general risk analysis of a typical federal agency with typical threats to typical vulnerabilities of typical information assets, and specified three security control baselines to address three levels of risk. The risk level—and subsequently the control baseline that should be selected—is determined when an agency categorizes the impact of a potential breach as low, moderate or high. This greatly simplifies the risk analysis process for federal agencies (see figure 5) and provides an “80 percent solution” for control specification.

Agencies are then expected to further tailor the baseline to ensure their unique information protection requirements are addressed. The tailoring process includes additional scoping to eliminate unnecessary controls, selecting compensating controls, assigning parameters for organization-defined parameters, adding controls and enhancements, and providing any additional information required for control implementation. This process can be used very granularly on a specific system or organizational element, or it can be used to create an overlay for general use, such as a general type of information system or organization.

Applying a framework-based approach to healthcare

Healthcare organizations can create their own overlay of a NIST SP 800-53 baseline by going through the tailoring process. While daunting for some organizations, it is arguably a more tractable approach than specifying a complete set of security controls based on a traditional risk analysis.

1. First, scale the controls by selecting an appropriate baseline from which to begin. This helps ensure time and effort is not wasted on implementing controls that aren’t necessary for the level of risk mitigation required.
2. Second, scope the scaled baseline by adding or enhancing controls, as needed, to address applicable regulatory, legal, contractual, and other business-related requirements unique to your organization. Controls may also be removed based on organizational and financial constraints; however, no control should be removed simply as a matter of convenience.
3. Third, specify compensating controls for baseline controls that cannot be implemented, e.g., due to technical, architectural, or financial reasons. Ensure the compensating controls address a similar type and amount of risk as the baseline controls.
4. Fourth, continue the tailoring process by reviewing the organization-defined parameters to ensure the values are consistent with best practices and industry due care and due diligence requirements.
5. And finally, review the resulting overlay periodically, or otherwise as needed, to ensure the overlay continues to address extant and emerging threats to your information assets.

The healthcare industry already leverages the overlay concept to great benefit. For example, the Centers for Medicare and Medicaid Services (CMS) produces an overlay of all three NIST SP 800-53 control baselines for their use and that of their contractors [4]. CMS also produces a separate overlay of the NIST SP 800-53 moderate control baseline for Health Insurance Exchanges [3]. And the Health Information Trust (HITRUST) Alliance produces an overlay of the NIST moderate baseline for the industry and incorporates mechanisms to help further tailor the overlay to an organizational type based on defined risk factors [9]. This approach is also used as the basis for Healthcare and Public Health Sector guidance [16] on implementing the NIST Cybersecurity Framework [14], published under the auspices of the Critical Infrastructure Protection Program.

Conclusion

Findings from the first round of OCR audits clearly indicate a traditional approach to risk analysis is difficult for many healthcare organizations. However, a controls-based framework such as the one provided by NIST can be leveraged by both public and private sector organizations to greatly simplify the risk analysis process. Such an approach helps ensure specification of a comprehensive and robust set of information security controls that complies with the HIPAA Security...
Rule and, more importantly, helps satisfy due care and due diligence obligations for the protection of sensitive patient health information.

References

About the Author
Bryan Cline, Ph.D., is a former CISO with 30 years of experience in information systems and cybersecurity in the public and private sectors. Cline is a private sector co-chair of the Joint HPH Cybersecurity WG, which produced the CIPAC-sponsored guidance on implementing the NIST Cybersecurity Framework in healthcare. He may be reached at bryan.cline@csps-infoprotect.com or @IA_Doctor.

Looking Ahead – December Journal
Social Media, Gaming, and Security; Due: 10/22/17
Based on 2016 statistics, 155 million Americans play online games regularly and 78 percent of the population has a social networking profile. With staggering numbers like this, these industries will probably thrive for the foreseeable future. Being interconnected with others in the community and around the world through these vehicles can be exciting but also poses numerous risks such as predators, addiction, identity theft, malware intrusion, and social engineering. These issues require both the vendors and consumers to become more vigilant to effectively protect themselves. Furthermore, tackling them can be complicated and time consuming and will inevitably impact this landscape. What research, experience, or best practices do you have to share in this area? The ISSA Journal is interested in hearing from you.

Submit articles to editor@issa.org.