Compliance Today - September 2022

Security risk management for the compliance officer

By Carol L. Amick

- linkedin.com/in/carolamick/

The security risk management program may not be the responsibility of the compliance officer; however, failure to ensure this required HIPAA control is in place could have negative impacts on your organization. Unidentified and unaddressed risks can easily lead to a loss of protected health information (PHI) or a bad actor taking over your entire system in a ransomware attack. A recent report by Sophos indicated that 66% of healthcare organizations had been hit with a ransomware attack.[1] Addressing security risks should be a top priority considering the U.S. Department of Health & Human Services (HHS) indicated in 2021 the average bill for rectifying a ransomware attack, including downtime, ransom, legal fees, etc., was $1.2 million.[2]

Including an evaluation of your security risk management process in your compliance plan will provide assurance to your leadership that while you may not be able to prevent all security incidents, your organization is at least making a consistent effort to reduce the risk.

Over the past 18 months there has been a lot of discussion about the need for healthcare organizations to perform cybersecurity risk assessments. There are probably several motivating factors behind these discussions and one of the primary drivers has been the passing of the HIPAA Safer Harbor Bill, HR 7898, which amended the HIPAA HITECH Act to require HHS to incentivize best practices in security.[3]

While HR 7898 was passed to provide incentives for good cybersecurity practices, the truth is that performance of an enterprise-wide risk assessment has long been a requirement for HIPAA compliance. A risk assessment has been required since the effective date of the HIPAA Security Rule in April 2005.

The standard within 45 C.F.R. § 164.308(a)(1)(ii)(A) [4] requires covered entities and business associates to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate." In 2018, the HHS Office for Civil Rights (OCR) provided guidance on their expectations for the implementation of this requirement, including:

- Does the entity have policies and procedures in place outlining compliance with this control?
- Has the entity conducted an "accurate and thorough assessment" of the potential risk and vulnerabilities?
- Does the risk analysis include:
  - A defined scope,
  - Details on identified threats and vulnerabilities,
  - An assessment of current security measures,
  - An impact and likelihood analysis, and

- A risk rating?[5]

So where are we now?

In 2020, 15 years after the effective date of the HIPAA Security Rule, the *2020 HIMSS Cybersecurity Survey* found that only 50% of the respondents were conducting comprehensive risk assessments. Organizations were often excluding key areas from their annual risk assessment (Table 1).[6]

Risk assessment component	Percent of respondents, including component
Email	58%
Legacy systems	45%
Mobile devices	39%
Cloud provider/service provider	37%

Table 1: Risk assessment components

This trend is particularly alarming when compared to the *2021 HIMSS Healthcare Cybersecurity Survey*, where 45% of respondents indicated that they had been the victim of phishing attack resulting in a significant security incident. A review of the initial point of compromise also points out the high risks for areas often excluded from an organization's annual risk assessment (Table 2).[7]

Initial point of compromise	Percent of significant security incidents
Phishing	71%
Legacy software	15%
Laptop, tablet, or device	10%
Legacy operating system	9%

Cloud provider/service	9%

Table 2: Initial point of compromise

The HIMSS survey is supported by a review of OCR enforcement actions for 2020 and 2021. In 80% of OCR press releases, there was failure to perform risk analysis. And, as previously noted, with the average $1.2 million price tag for rectifying a ransomware attack, addressing security risks is a top priority.[8]

Including an evaluation of your security risk management process in your compliance plan will provide assurance to your leadership that while you may not be able to prevent all security incidents, your organization is at least making a consistent effort to reduce the risk.