SE130196-Vũ Hoàng

Discussion 3:

Case Study: Information Security Risk Assessment for a  
Small Healthcare Clinic Using the Security Risk  
Assessment Tool Provided by HealthIT.gov

Abstract

Information security risk assessments in the healthcare industry are legally required and demand an ongoing investment of time and resources

Introduction

The Security Risk Assessment (SRA) Tool provided by HealthIT.gov is designed to meet this challenge for healthcare companies of all sizes and (CSP) as the primary method to handle patient ePHI, aim to advance the interests of all parties to more effectively manage these risks by moving towards best practices and compliance with the HIPAA Security Rule

2.Review of Literature

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014) is the current broad information security standard in this area (Paulsen & Toth, 2016) The Balridge Cybersecurity Excellence Builder (NIST, 2016) is a self-assessment tool provided by NIST which gives organizations the ability to invest their time on a targeted basis to better understand their information security risk posture

The Department of Health and Human Services (HHS) provides compliance information specific to HIPAA and the cloud Understanding data loss prevention (DLP) and its associated technologies can provide

important insight and benefits to safeguarding ePHI. Beeskow (2015) notes three primary considerations related to DLP: where confidential data is stored, who is accessing the information, and how data is being handled. Another important element within healthcare is the inherent conflict of interest between protecting the patient and protecting their data No survey of current information security efforts in healthcare would be complete without mention of the Health Information Trust Alliance (HITRUST) Common Security

Framework (CSF)

(HITRUST, 2017) is a top-level industry standard created and managed in partnership between many of the largest healthcare providers and can be applied to organizations of varying size useful industry perspective, which is built around HIPAA compliance, is the HIPAA Journal In any case, a significant ongoing time and energy investment is required to ensure that the overall process is managed well.

\* The HITRUST CSF is organized by 14 Control Categories, which contain 46 Control Objectives and 149 Control Specifications based on ISO/IEC 27001:2005 and 27002:2005. Each Control Specification consists of as many as three implementation levels applied to healthcare organizations according to specific organizational, system and regulatory factors

3. Methodology

According to HIMSS (2016), the most recently updated version of the SRA Tool streamlines the ability of small healthcare providers to comply with the HIPAA SecurityRule

4. Results & Recommendations

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

All information entered into the SRA Tool is stored locally to the users’ computer or tablet. HHS does not receive, collect, view, store or transmit any information entered in the SRA Tool. The results of the assessment are displayed in a report which can be used to determine risks in policies, processes and systems and methods to mitigate weaknesses are provided as the user is performing the assessment. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.It is useful, though it has some drawbacks

\* Backend-as-a-Service (BaaS) is a cloud service model in which developers outsource all the behind-the-scenes aspects of a web or mobile application so that they only have to write and maintain the frontend. BaaS vendors provide pre-written software for activities that take place on servers, such as user authentication, database management, remote updating, and push notifications (for mobile apps), as well as cloud storage and hosting.

\* **Content Security Policy** ([CSP](https://developer.mozilla.org/en-US/docs/Glossary/CSP)) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting ([XSS](https://developer.mozilla.org/en-US/docs/Glossary/XSS)) and data injection attacks

\* SFA is the set of DoD activities that support the development of the capacity and capability of foreign security forces and their supporting institutions

\* DRP is a plan for business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data records and the physical space of an organization

\*CP is Check Point and other meanings are located at the bottom which take place within Security terminology

5.Discussion

The CloudTrust Protocol is an additional mechanism that

could bring greater clarity in this area through future work. (Cloud Security Alliance, n.d.) wonders at what point consumers will start demanding better information security practices en masse from various healthcare providers. Stalled federal legislation such as the Transparent Ratings on Usability and Security to Transform Information Technology (TRUST IT) Act of 2015 may need to be re-examined to give consumers more information regarding healthcare organizations which fail to prioritize the protection of their data. (Leventhal, 2015)

6.Conclusion

Demonstrates due diligence which will minimize the impact of a data breach or audit. Information security is a moving target and requires periodic assessment and analysis to keep up with the changes. Only a proper prioritization of time and resources will ensure that small healthcare clinics, such as the one featured in this case, do not fall behind.