medisked

Stay Safe: Cybersecurity Best Practices

The National Institute of Standards and Technology (NIST) defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." As part of cybersecurity, organizations should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks.

This white paper highlights security program best practices that have been designed to protect organizations from cyber-attacks as well as information assets and business resilience.

The Federal Financial Institutions Examination Council (FFIEC) recommends organizations consider taking the following steps:

1. Conduct Ongoing Information Security Risk Assessments

The Security Office should develop and implement systems or tools for assessing the security and privacy impacts of all new and existing systems and programs. The first step is to perform a security risk assessment to determine: whether an activity involves PHI/PII or otherwise may impact privacy, whether a more robust Security Risk Assessment is required, and if an existing system of record covers a specific information classification. The security risk assessment is also a way for the organization to ensure that privacy is considered in systems undergoing development, and in determining the security categorization of a system based on the potential impact to the organization or individuals should there be a breach of security.

Organizations may elect to perform self-assessments of activities involving regulated data to ensure compliance with privacy laws, regulations, internal policies, and any other established privacy controls. The assessments may encompass an entire business process or focus on a single information system or vendor processing the data. An assessment project may involve documenting the people, processes, and technologies affecting the flow and use of PII/PHI, as well as performing a legal and policy gap analysis and providing a mitigation strategy. The resulting assessment report is useful for providing management and the Security Office with key insights into business activities requiring further scrutiny for security or privacy issues.

2. Securely Configure Systems and Services

Organizations covered by HIPAA are required to implement, test, and monitor specific management, operations, and technical controls to protect healthcare information. NIST SP 800-53, Security and Privacy Controls for Information Systems, establishes common criteria for assessing the effectiveness of security controls in information systems. Organizations use the recommended assessment procedures from NIST SP 800-53 to develop their own assessment procedures. Organizations report annually on specific privacy and security activities in their annual HIPAA Risk Assessment reports to senior leadership and the BOD.

3. Protect Against Unauthorized Access

The Security office can provide expertise in support of the organization's efforts to use privacy enhancing technologies to mitigate information security risks. For example, organizations should review and implement, to the maximum extent practicable, automated solutions, such as encryption and data loss prevention (DLP) technologies that prevent inadvertent exposure of PII in storage or transmission. Encryption technologies that meet NIST requirements have been used for years to protect PII maintained in data bases or on mobile devices and when transferring data across the Internet. Implementation of this technology should be reviewed to be complete across an organization.

4. Perform Security Monitoring, Prevention, and Risk Mitigation

The Privacy Act expressly requires that PII be secured. Once an organization approves a policy decision to collect and use PII for a specific authorized purpose, the Security & Privacy Office is responsible for implementing comprehensive policies and procedures to ensure the confidentiality, integrity, and availability of that data. The Security & Privacy Office is responsible for establishing requirements, including the use of appropriate technologies, for privacy-related data management.

5. Update Information Security Awareness and Training Programs to Include Cyber-Attacks

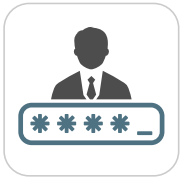
Security training and awareness programs are key elements of building a culture of data protection throughout an organization. Training programs test and reinforce the implementation of security and privacy policies, providing a critical element of an effective security program. The Compliance Office has primary responsibility for ensuring that employees and contractors receive mandated security and privacy training. Training and awareness programs can provide valuable feedback to help refine and improve security management and reduce the risk of incidents throughout the organization.

6. Implement and Regularly Test Controls Around Critical Systems

It is vital that organizations incorporate security and privacy risk mitigation in the earliest project and lifecycle planning stages, providing project managers with the opportunity to build security and privacy directly into processes and tools. Integrated security and privacy controls are more effective, easier to maintain, and typically have lower lifecycle costs. The Security Office is responsible for identifying various ways to embed security into these SDLC processes. This can be done through integration with the organization Project Management Office milestone or gate reviews.

7. Review, Update, and Test Incident Response and Business Continuity Plans Periodically

HIPAA requires organizations to develop and maintain an incident response policy and notification plan. Even with the implementation and monitoring of privacy and security controls, it is impossible to prevent all risks associated with IT operations. Being prepared to respond to and mitigate these risks before substantial damage is done is critical to the success of a security program. Test the Incident Response Plan through a tabletop exercise where all key stakeholders participate in walking through an incident with associated responses documented. Evaluate the responses to confirm that legal and regulatory requirements are met through the procedures.



8. Centralize Identify and Access Management

Having multiple disjointed authentication systems can be a burden on an organization and its users. This reduces an organization's ability to maintain security best practices and compliance. Organizations with a single authentication system, such as Active Directory, will be better prepared to follow the NIST SP 800-53 guidelines than organizations attempting to manage many different authentication systems. Risk is reduced in a centralized model by granting system access according to one interpretation of policy and less complexity involved in user creation, modification, and access auditing. Centralizing identity and access management within one system that provides authentication to all applications and resources can greatly improve an organization's security posture.

9. Participate in Industry Information-Sharing Forums

When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the Healthcare Information Sharing and Analysis Center (H-ISAC) worldwide receive timely notification and authoritative information specifically designed to help protect critical systems and assets from cyber and physical security threats. You can get more information on the NH-ISAC organization at https://nhisac.org/

This is a good list of security program best practices, but not one that is easily and readily implemented in the short-term. These practices should be implemented in a defense-in-depth manner which helps control risk across the organization.