Barbara Garcia

05/06/2024

**D486 – Governance, Risk, and Compliance Performance Assessment**

**A. Security Gaps According to SAR**

Upon reviewing the Security Assessment Report for Fielder Medical Center, various security gaps exist in the company’s existing security framework. These gaps include inadequate protection for personally identifiable information, workstations with unacceptable or nonexistent antivirus solutions, inadequate endpoint protection, lack of multi-factor authentication, and a firewall that is end of life. As to internet infrastructure, the database containing PII is directly accessible to the web instead of being located on a screened subnet as it should be and there is no encryption directly between the server and the portal that doctors and government employees use to access the database. With the new digitization system, there is no secure process to authenticate doctors on the network or to upload PII and other artifacts to the system.

**B. Five Controls in 3.3 of SAR**

The five security controls identified in section 3.3 of the SAR are least privilege, plan of action and milestones, continuous monitoring, risk assessment and risk response.

**B1. Associated Risk Rating**

**1. Least Privilege**

The risk associated with this control is elevation of privilege. The risk rating is high because if an unauthorized person can gain access to privileged accounts, it can result in loss of confidentiality, integrity, and availability of sensitive data, including personally identifiable information. In addition to business risks such as loss of reputation and financial loss, this risk can result in fines and potentially criminal charges.

**2. Plan of Action and Milestones**

The risk associated with this control is unmitigated vulnerabilities. The risk rating is medium. This control aims to, “correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system (“CA-5: Plan of Action and Milestones - CSF Tools”).” Leaving known vulnerabilities un-addressed opens the entire network including sensitive data to attack.

**3. Continuous Monitoring**

The risk associated with this control is an attack going unnoticed due to lack of monitoring. The risk rating is high because if the network is not monitored and an attack attempt, or an attack occurs, the IT Security team will not be able to respond and stop the attack before sensitive data, is leaked, changed, or made unavailable.

**4. Risk Assessment**

The risk associated with this control is unidentified vulnerabilities. The risk rating is high. Since the system deals with sensitive data, failure to identify vulnerabilities introduced by the system puts confidentiality, integrity, and availability of data at risk.

**5. Risk Response**

The risk associated with this control is incorrect prioritization of mitigation strategies. The risk rating is medium because of the Potential to put too much focus on lower rated risks instead of focusing remediation efforts on mitigating risks that would cause more damage if acted upon.

**B2. Justification for Chosen Remediation**

**1. Least Privilege**

Accepting the risk of privilege escalation would not be an acceptable risk due to the sensitivity of the data (PII), desire of the company to process credit card transactions (PCI DSS), and the compliance requirements that apply to the company due to them working with the government (FISMA).

**2. Plan of Action and Milestones**

Given the company contracts with the federal government and are therefore obligated to comply with FISMA, they cannot accept the risk of not developing a plan of action and milestones. Per the NIST CSF Tool, “Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB (“CA-5: Plan of Action and Milestones - CSF Tools”).”

**3. Continuous Monitoring**

To comply with its business requirements, the company cannot accept the risk of not implementing a continuous monitoring program. “Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions (“CA-7: Continuous Monitoring - CSF Tools”).” In the absence of a continuous monitoring program, if a threat actor were to successfully gain access to the system, it would likely go unnoticed resulting in no incident response being initiated and the resulting harm to the business, clients and partners would be exponentially worse.

**4. Risk Assessment**

An essential part of risk assessment is to, “consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers and outsourcing entities (“RA-3: Risk Assessment - CSF Tools”).” The company works with various external parties making it essential to mitigate the risk of unidentified vulnerabilities. Accepting this risk would leave the company vulnerable to attack and out of compliance with regulatory requirements.

**5. Risk Response**

Risk response is essential in addressing the risk of mis-prioritizing mitigation strategies. “Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry (“RA-7: Risk Response - CSF Tools”).” The potential to prioritize mitigation strategies for lower risk vulnerabilities above critical vulnerabilities can leave sensitive data at risk due to limited resources.

**C. How to Remediate**

**1. Least Privilege**

The remediation for this is to implement a strong password policy and multi-factor authentication. Assets to implement this remediation are an app with a security token to use for authentication in addition to strong passwords. Action that needs to be taken is company management and IT team work together to create policies for secure passwords and use of multi-factor authentication. Changes to be implemented include the use of logical controls to implement multi-factor authentication when accessing company data, especially sensitive data and to use logical controls to enforce password complexity, password length, and regular password changes.

**2. Plan of Action and Milestones**

Remediation for the related risk is to develop a plan of action with clear milestones and track planned remediation actions. The asset needed is the existing plan of action and milestones for the company. Actions needed include to update the plan of action and milestones to reflect “findings from security controls assessments, security impact analyses, and continuing monitoring activities (“CA-5: Plan of Action and Milestones - CSF Tools”).” Findings should reflect the updated system after new digitization tools have been implemented. Changes include updating the plan of action and milestones appropriately.

**3. Continuous Monitoring**

The remediation for the related risk is continuous monitoring. Assets needed include a SIEM (Security Incident and Event Monitoring) solution, IDS (Intrusion Detection System), firewall and security operation center staff (or contracted MSSP). The action item is for staff to be assigned to continuously monitor and respond events aggregated to the SIEM. Changes include to install intrusion detection devices on each endpoint, install a stateful firewall, and set up logs to be forwarded to a central SIEM.

**4. Risk Assessment**

The remediation for the related risk is risk assessment. Assets needed to complete this mitigation are IT leadership and company leadership. The action needed is to conduct a risk assessment that identifies the threats and vulnerabilities in the system, determines the likelihood, magnitude and harm from a security breach, and “determine the likelihood and impact of adverse events on individuals arising from the processing of personally identifiable information (“RA-3: Risk Assessment - CSF Tools”).” The change needed is to update the current risk assessment.

**5. Risk Response**

The remediation for the related risk is risk response. The assets needed to implement the mitigation are the compliance documents for PCI DSS, FISMA, and HIPAA. The action that needs to be taken is to, “respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance (“RA-7: Risk Response - CSF Tools”).” The change needed is to use compliance documentation as a guide to implement appropriate security controls for each risk.

**D. PCI DSS Compliant Policies**

The SAR makes three recommendations to aid in developing policies that comply with the Payment Card Industry Data Security Standard: Maintain a secure network with a firewall, remove vendor-supplied default passwords and configurations, and install an antivirus solution.

To establish and maintain a secure network with a firewall, the role to implement the change will be the IT and Cybersecurity teams. Responsibilities include to design a secure network with fully patched hardware and software, implement firewall rules that comply with PCI DSS standards, use VPN for third parties to access the server, use host and network-based IDS solutions, implement a SIEM that is regularly monitored, isolate servers containing sensitive information in a screened subnet, enable encryption for data at rest and data in transit, and implement configuration management for all devices, network components and software.

To remove vendor-supplied default passwords and configurations, the role will be allocated to the IT department. Responsibilities include to enforce strict password policies and configure devices according to CIS benchmarks.

For implementing an antivirus solution, the role will be allocated to the IT department and the responsibilities include to install an up-to-date antivirus solution on each endpoint, properly configure and regularly update the antivirus solution, and monitor the antivirus solution to react quickly to potential threats.

**Works Cited**

AC-6: Least Privilege - CSF Tools. (2021, March 5). Csf.tools. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-6/

‌ https://csrc.nist.gov/files/pubs/fips/199/final/docs/fips-pub-199-final.pdf.

“CIS BenchmarksTM.” CIS, www.cisecurity.org/cis-benchmarks.

‌“CA-5: Plan of Action and Milestones - CSF Tools.” Csf.tools, 13 Aug. 2020, csf.tools/reference/nist-sp-800-53/r4/ca/ca-5/.

“CA-7: Continuous Monitoring - CSF Tools.” Csf.tools, 13 Aug. 2020, csf.tools/reference/nist-sp-800-53/r4/ca/ca-7/.

“RA-3: Risk Assessment - CSF Tools.” Csf.tools, 5 Mar. 2021, csf.tools/reference/nist-sp-800-53/r5/ra/ra-3/.

“RA-7: Risk Response - CSF Tools.” Csf.tools, 5 Mar. 2021, csf.tools/reference/nist-sp-800-53/r5/ra/ra-7/.

*‌*