12_Analyzing_OpenMRS_Risks_&_What_To_Do_About_Them |-100_Days_Of_GRC

Task:

Take a few risks from your brainstorm list (at least 3) and *assess them*. For each risk scenario, quickly note a Likelihood (High/Med/Low) and Impact (High/Med/Low). Then decide on an action: Mitigate, Avoid, Transfer, or Accept (or a mix). Write a one-liner for each with those elements. For example: *"Risk of patient data leak via lost backup drive – Likelihood Low, Impact High, so risk = Medium; Response: Mitigate by encrypting backups, Transfer residual risk via cyber insurance."* This practice will help solidify the thought process of ranking and responding to risks. Keep it simple – no need for perfection on scoring, just make reasoned guesses.

Answer:

Risks

1. **Man-in-the-Middle (MitM) Attack.** If network traffic between OpenMRS clients and servers is not properly encrypted, attackers on the same network could intercept, alter, or steal sensitive data in transit.

Likelihood – M. Impact – High. **Response** – **Mitigate**: Ensure that strong network segmentation and encryption controls are in place. Use VPNs or secure tunnels for remote access to OpenMRS. Implement network segmentation to isolate OpenMRS traffic from untrusted networks. Monitor for suspicious network activity and regularly audit and test encryption configurations to ensure they remain secure. **Transfer:** i.e., cyber insurance can be considered for residual risk, but it obviously does not replace technical controls. **Accept:** this would only be appropriate for any minimal residual risk after all reasonable mitigations are in place.

2. **Insider data misuse.**

Likelihood – M. Impact – High. **Response**: **Mitigate**. Insider threats are persistent and very hard to avoid because insiders have legitimate access to systems and data. Have strong access controls such as least privilege and RBAC, and ensure strong authentication multi-factor authentication, credential rotation as well. Monitoring and auditing (user activity logs, anomaly detection). Employee education and awareness (regular training, phishing simulations).

Comprehensive security policies (data handling, incident response). Ensure zero trust architecture (continuous verification, micro-segmentation). **Transfer** and **Accept** can be used for residual risk only after implementing strong controls.

3. **Power outage.**

Likelihood – L. Impact – High. Response – Mitigate: Use AWS multi-region or multi-availability zone deployments to reduce single points of failure, thereby creating redundancy. Implement strong backup and disaster recovery plans. Document and train staff on downtime procedures for clinical continuity. Monitor AWS service health and set up alerts for outages. **Transfer**: Consider business interruption or cyber insurance to offset financial risk from rare but possibly impactful outages. **Accept**: After implementing strong controls, accept the small residual risk that cannot be fully eliminated.

4. **Hackers** on the internet could target patient data and malware could infect the system, or a ransomware attack could attempt to encrypt the OpenMRS database.

Likelihood – H. Impact – High. **Mitigate**: Encrypt data at rest and in transit. Regularly patch and update OpenMRS and all dependencies. Deploy endpoint protection and anti-malware tools.

Use AWS security services: GuardDuty, CloudTrail, Security Hub, and automated monitoring for suspicious activity. Backup data regularly and test recovery procedures. Prepare and rehearse incident response plans. **Transfer**: Consider cybersecurity insurance to offset financial risk. **Accept**: After implementing robust controls, accept the small residual risk that cannot be fully eliminated.

Reflection Prompt:

Think about **Risk Tolerance**: Are there any risks you would be willing to **accept** for OpenMRS, and why? In other words, which risks seem minor enough that you'd say, "We can live with that," especially given limited resources. Understanding what you're willing to accept versus what you must address is key in risk management. Reflect on your comfort level with risk – it's a very personal and organizational thing!

Answer:

Risks I'm willing to accept for OpenMRS

1. **Insider Threats from Low-Access Users**
   I would be willing to accept low-level insider risk for staff with minimal data access to non-sensitive fields.
2. **Low-Likelihood Infrastructure Risks such as Power Outages and/or Natural Disasters.** I think I could accept the residual risk of AWS infrastructure failures because I can implement multi-region deployment and backup procedures. Plus, AWS's track

record shows these events are rare. Moreover, the cost of eliminating all residual risk may exceed the benefit. At a certain point, further investment will yield diminishing returns, so once I've implemented standard mitigations like multi-region failover, documented downtime procedures, and regular backup testing, I would be comfortable accepting this risk.