Course Project: Audit Checklist

Damien Beltran | Hannah Stanek | Isaiah Alvarez | Wes Gause
CS-3113-01T

About the Audit

This cybersecurity audit will be an overview of NAROs digital defense systems. It will identify your organization's vulnerabilities, ensure that your data is protected, and will aid you in following the industry standard. At Death StarConsulting, our audits are made with no formal IT background in mind to maintain simplicity while possessing real world use, allowing for easy understanding and exemplary results.

Identify

1. Do you have a list of employees and volunteers with access to systems or sensitive data?
   (Yes / No / Not Sure)

2. Do you have a list of all electronic devices used at your organization?
   (Yes / No / Not Sure)

3. Have you identified which data is most important to your organization (e.g., donor records, financial info)?
   (Yes / No / Not Sure)

4. Are user accounts set up so that each person has their own login?
   (Yes / No / Not Sure)

5. Which users in your organization have administrative privileges or are members of an administrative group?

   _____

6. Do you have designated roles for who manages cybersecurity and IT (even if outsourced)? (Yes / No / Not Sure)

7. Are vendors and 3rd parties monitored for security risks and vulnerabilities?
   (Yes / No / Not Sure)

8. Is your company required to maintain any legal or regulatory compliance (HIPAA, PCI-DSS)?
   (Yes / No / Not Sure)

9. Are your servers located in a secure room within your facility with restricted access. If so, who has access to the room?
   (Yes / No / Not Sure)

10. Are staff and volunteers trained on how to spot phishing emails or scams?
    (Yes / No / Not Sure)

11. How often is your inventory reviewed and updated?

    _____

12. Do you have a policy outlining acceptable use of organizational technology?
    (Yes / No / Not Sure)

Protect

13. Do you use multi-factor authentication (MFA) for important accounts (email, banking, etc.)?
    (Yes / No / Not Sure)

14. Are devices updated on a regular basis?
    (Yes / No / Not Sure)

15. Does your organization use Web Application Firewalls (WAFs) or other endpoint protection devices?
    (Yes / No / Not Sure)

16. Do you place restrictions on allowed internet sites or SPAM filtering?
    (Yes / No / Not Sure)

17. Are backups completed on a regular basis? If so, are they protected with encryption?
    (Yes / No / Not Sure)

18. Are backups stored separately from your main system (cloud or external)?
    (Yes / No / Not Sure)

19. Does your company use encryption when storing or transmitting sensitive files?
    (Yes / No / Not Sure)

20. Do you allow the use of removable media such as USB devices?
    (Yes / No / Not Sure)

21. Do you require strong passwords (e.g., 12+ Characters, Number, Upper Case and Lower Case characters, symbol, etc.)
    (Yes / No / Not Sure)

22. Is all software (including operating systems) kept up to date?
    (Yes / No / Not Sure)

23. Is there a secure coding policy guiding developers?
    (Yes / No / Not Sure)

24. Are your servers located in a secure room within your facility with restricted access. If so, who has access to the room?

25. Do you use antivirus or anti-malware software on all computers?
    (Yes / No / Not Sure)

26. Is there a procedure for offboarding employees that has been terminated in a timely manner?
    (Yes / No / Not Sure)

27. Is there any security procedure or training that is performed when onboarding new employees?
    (Yes / No / Not Sure)

28. Do mobile devices and laptops support remote wiping?
    (Yes / No / Not Sure)

Detect

29. Have you enabled alerts or notifications for unusual login attempts?
    (Yes / No / Not Sure)

30. Are external connections, such as remote desktop or VPNs allowed and are they monitored?
    (Yes / No / Not Sure)

31. Is there anyone that monitors the logs that are generated for your network and devices?
    (Yes / No / Not Sure)

32. Do you have any automated tools that scan for malware or unusual activity?
    (Yes / No / Not Sure)

33. Do you periodically assess your systems for unauthorized software installations?
    (Yes / No / Not Sure)

34. Do you audit user accounts for suspicious activity on a regular basis?
    (Yes / No / Not Sure)

35. Do users know how to report unusual activity (like strange emails or system behavior)?
    (Yes / No / Not Sure)

Respond

36. Is there a response plan for data breaches, including notification procedures?
    (Yes / No / Not Sure)

37. Are records of incidents and your response actions documented and stored securely?
    (Yes / No / Not Sure)

38. Is there a documented and regularly updated incident response plan?
    (Yes / No / Not Sure)

39. Are staff trained on their roles in incident response processes?
    (Yes / No/ Not Sure)

40. Have you practiced what to do in the event of a cyber incident (a "tabletop" exercise)?
    (Yes / No / Not Sure)

41. Is your incident response plan updated based on lessons learned from previous incidents?
    (Yes / No / Not Sure)

Recover

42. Is there a plan for post-incident recovery and system restoration in case of compromise?
    (Yes / No / Not Sure)

43. How often and what types of backups are currently performed at your organization. (Full backups, incremental, hourly, daily, weekly)?

    _____

44. Have you tested your ability to restore from a backup?
    (Yes / No / Not Sure)

45. Do you have cyber insurance?
    (Yes / No / Not Sure)

Review Summary

- Total - Yes: _____ No: _____ Not Sure: _____

- Priority Follow-ups:

1.
2.
3.