**Submissions (in softcopy only):**

* Submit a softcopy of your handwritten notes on GCR.
* Submit the threat and risk assessment of the selected industry e.g., Daraz, Alibaba, Meezan Bank etc. and propose the risk/threat mitigation approaches against the specific attacks/threat/risk towards the company. (with the help of 70 questions pdf file)

**Training**

1. Do you conduct robust and frequent end-user cybersecurity awareness training?

- Limited training due to resource constraints.

2. Have you taught everyone how to securely store passwords or passphrases?

- Training provided, but enforcement challenging across diverse systems.

3. Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?

- No, frequency is lower due to operational challenges.

4. Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors, and how to report any suspicious activities for further investigation?

- Awareness is not universal; reporting procedures may lack clarity.

**Access Control**

5. Are all vendor default accounts changed or disabled?

- Changes not consistently applied across systems.

6. Are only necessary services, protocols, daemons, and functions enabled?

- Disabling unnecessary functions is challenging.

7. Is all unnecessary functionality removed or disabled?

- Removal restricted due to dependencies.

8. Are all accounts immediately disabled or deleted upon termination of employment?

- Delays may exist in disabling accounts.

9. Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?

- Uniform implementation challenging.

**End User**

10. Do you provide end users a tool to save all passwords (preferably cloud-based for home and work use)?

- Tools for password management not uniformly provided.

11. Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?

- Policies not consistently enforced.

**End Points**

12. Are all endpoint logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?

- Limited integration of advanced threat intelligence.

13. Do you harden all endpoints and remove everything that is not needed for job functionality?

- Complete hardening challenging.

14. Do you have next-generation anti-malware protection on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?

- Implementation limited due to compatibility issues.

15. Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your network?

- Limited control over non-enterprise devices.

16. Do all endpoints have personal firewalls for accessing the Internet when not attached to the enterprise network?

- Personal firewalls may not be uniformly implemented.

17. Do all endpoints have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?

- Uniform antivirus implementation challenging.

18. Do all endpoints have a next-generation anti-malware application installed?

- Limited implementation due to compatibility.

**Event Management**

19. Are all logs stored for at least 2 years?

- Log storage duration may vary.

20. Are all devices generating logs?

- Logging capabilities may not be uniform.

21. Are all logs being reviewed daily by inside and/or outside sources?

- Daily log reviews challenging.

22. Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?

- Incident response may be constrained.

**Security Architecture**

23. Do you only give employees the tools and access needed to perform their job functions, and nothing else?

- Access control challenging due to tool dependencies.

24. Do you utilize the principle of least privilege?

- Least privilege challenging to enforce uniformly.

25. Do you deploy a zero-trust model?

- Implementation limited.

26. Do you require multifactor authentication (MFA) for all connections outside of the network?

- MFA implementation challenging for external connections.

27. Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?

- MFA enforcement may vary for internal access.

28. Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)

- Credential management efficiency may vary.

29. Have you recently assessed your Active Directory to ensure that it is properly configured and secured?

- Regular assessments may face challenges.

30. Are you actively monitoring the security of your Active Directory?

- Active monitoring may be limited.

31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?

- Firewall rules may vary.

32. Is your demilitarized zone (DMZ) secured?

- Securing the DMZ is challenging.

33. Has it been ensured that there are no data, databases, or stored accounts on the DMZ?

- Ensuring a data-free DMZ is challenging.

34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?

- Anti-spoofing technology deployment may vary.

35. Do you prevent the disclosure of internal IP address and routing information on the Internet?

- Preventing disclosure may face challenges.

36. Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting WiFi, confidential data, virtual machines, and printers away from crown jewels)?

- Segmentation may be limited.

**Cryptography**

37. Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?

- Implementation of key protection measures may vary.

38. Are cryptographic keys stored in the fewest possible locations with at least dual custodians?

- Key storage practices may face challenges.

39. Do you utilize full disk encryption on all appropriate drives?

- Full disk encryption may not be universally implemented.

40. Do you use secure encryption in motion—at least Transport Layer Security (TLS) 1.1 or higher?

- Secure encryption standards may vary.

41. Is all non-console administrative access encrypted using strong cryptography?

- Consistent encryption may face challenges.

**Threats**

42. Do you perform periodic targeted threat hunts?

- Limited periodic threat hunts may be conducted.

43. Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?

- Threat intelligence integration may be limited.

44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?

- Routine dark web reconnaissance may face challenges.

45. Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?

- Monitoring vendor connections may vary.

**Testing**

46. Do you conduct at least 1 penetration test annually, performed by a third party?

- Annual third-party penetration testing may be limited.

47. Do you conduct routine vulnerability scans and remediate all vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?

- Routine scans and timely remediation may face challenges.

48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?

- Routine scanning may be limited.

49. Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?

- Annual risk analysis reports may face challenges.

**Policy**

50. Do you have an enterprise security policy that is updated at least annually and understood by all parties to which it applies?

- Updating and universal understanding may face challenges.

51. Do you have a formal change control policy?

- Formal change control policies may vary.

**Physical**

52. Are processes and mechanisms for restricting physical access to servers, consoles, backup, and network equipment in place and properly safeguarded?

- Physical access restrictions may vary.

53. Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?

- Controls on network jacks may face challenges.

**Plans**

54. Do you have a good cyber incident response plan (CIRP) that is reviewed and practiced yearly? The CIRP should be routinely updated, and the core and extended incident response teams should practice responses at least annually using tabletop or functional cybersecurity exercises.

- Incident response planning and practice may be limited.

55. Do you have playbooks with technical instructions for handling common cybersecurity incidents?

- Playbooks for incidents may face challenges.

**Inventory**

56. Do you have thorough diagrams of the entire network, including Wi-Fi?

- Thorough network diagrams may vary.

57. Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners, and restoration? Does this inventory include instructions with time periods to recover?

- Complete asset inventories may be challenging.

58. Do you have a full set of data flow diagrams?

- Full data flow diagrams may face challenges.

**Data Management**

59. Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?

- FIM of critical data may vary.

60. Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?

- Storage practices for confidential data may face challenges.

61. Do you require data classification throughout the network?

- Universal data classification may be challenging.

62. Do you deploy a network and cloud-based data loss prevention (DLP) program anywhere confidential data reside?

- DLP deployment may vary.

63. Do you prevent confidential data from being copied to external devices and external devices from being attached to endpoints?

- Preventing data copying may face challenges.

**Software Development**

64. Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?

- Secure software development practices may be limited.

65. Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?

- Universal adoption of prevention techniques may be challenging.

66. With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?

- Ongoing addressing may be limited.

67. Are these applications protected against attacks?

- Protection against attacks may vary.

68. Are preproduction environments separated from production environments, and is separation enforced with access controls?

- Separation may face challenges.

**Mobile Devices**

69. Are all mobile devices governed by effective mobile device management (MDM) policies?

- Mobile device governance may vary.

70. Do you disallow any connectivity of mobile devices not controlled by enterprise security mechanisms?

- Disallowing connectivity may be challenging.