Cybersecurity Assessment for Avanza Solutions

70 Layers of Defense

**Training**

Q1: Do you conduct robust and frequent end-user cybersecurity awareness training?

A: Yes, but with limited resources. Regular training is conducted, but budget and staffing constraints limit the scope and frequency

Q2: Are all vendor default accounts changed or disabled?

A: No, changes are not consistently applied across systems.

Q3: Do you provide end users a tool to save all passwords (preferably cloud-based for home and work use)?

A: No, tools for password management are not uniformly provided.

Q4: Do you harden all endpoints and remove everything that is not needed for job functionality?

A: No, complete hardening is challenging.

**Access Control**

Q5: Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your

network?

A: No, limited control over non-enterprise devices.

Q6: Do you require multifactor authentication (MFA) for all connections outside of the network?

A: Yes, but with limited MFA implementation for external connections.

Q7: Do you perform periodic targeted threat hunts?

A: Yes, but with limited frequency.

Q8: Do you conduct at least 1 penetration test annually performed by a third party?

A: No, annual third-party penetration testing is limited.

Q9: Are all mobile devices governed by effective mobile device management (MDM) policies?

A: No, mobile device governance varies.

**End User**

Q10: Do you have a good cyber incident response plan (CIRP) that is reviewed and practiced yearly?

A: No, incident response planning and practice may be limited.

Q11: Have you taught everyone how to securely store passwords or passphrases?

A: Yes, but enforcement is challenging across diverse systems.

**End Points**

Q12: Are only necessary services, protocols, daemons, and functions enabled?

A: No, disabling unnecessary functions is challenging.

Q13: Are all accounts immediately disabled or deleted upon termination of employment?

A: No, there may be delays in disabling accounts.

Q14: Are all endpoint logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI)?

A: No, limited integration of advanced threat intelligence.

Q15: Are all devices generating logs?

A: No, logging capabilities may not be uniform.

Q16: Do you utilize the principle of least privilege?

A: No, least privilege is challenging to enforce uniformly.

Q17: Are procedures defined and implemented to protect cryptographic keys used to protect stored data?

A: No, implementation of key protection measures may vary.

Q18: Do you conduct routine vulnerability scans and remediate all vulnerabilities timely?

A: No, routine scans and timely remediation face challenges.

**Event Management**

Q19: Are processes and mechanisms for restricting physical access to servers and network equipment in place?

A: No, physical access restrictions may vary.

Q20: Do you have a complete inventory of all assets that includes business criticality levels and owners?

A: No, complete asset inventories may be challenging.

Q21: Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?

A: No, the frequency is lower due to operational challenges.

Q22: Does everyone in your organization understand the risk associated with cybersecurity?

A: No, awareness is not universal; reporting procedures may lack clarity.

**Security Architecture**

Q23: Is all unnecessary functionality removed or disabled?

A: No, removal is restricted due to dependencies.

Q24: Are all screen idle times set for 15 minutes and require reauthentication to unlock?

A: No, uniform implementation is challenging.

Q25: Do all endpoints have next-generation anti-malware protection?

A: No, implementation is limited due to compatibility issues.

Q26: Do you manage all credentials in a manner that allows quick password reset for every account?

A: No, credential management efficiency may vary.

Q27: Do you deploy a zero-trust model?

A: No, implementation is limited.

Q28: Do you prevent the disclosure of internal IP address and routing information on the Internet?

A: No, preventing disclosure faces challenges.

Q29: Do you utilize full disk encryption on all appropriate drives?

A: No, full disk encryption is not universally implemented.

Q30: Do you have a formal change control policy?

A: No, formal change control policies may vary.

Q31. Do you have next-generation anti-malware protection on all endpoints?

A: No, implementation is limited due to compatibility issues.

Q32. Do you prevent confidential data from being copied to external devices?

A: No, preventing data copying faces challenges.

Q33: Do you require data classification throughout the network?

A: No, universal data classification is challenging.

Q34: Do you ingest current threat intelligence from more than one source?

A: No, threat intelligence integration is limited.

Q35:Do you perform routine dark web reconnaissance about your brand and enterprise structures?

A: No, routine dark web reconnaissance faces challenges.

Q36: Do you monitor all vendor and third-party supply-chain connections for compliance?

A: No, monitoring vendor connections varies.

Q37: Do you conduct routine vulnerability scans and remediate vulnerabilities timely?

A: No, routine scans and timely remediation face challenges.

Q38: Do you have an enterprise security policy updated at least annually?

A: No, updating and universal understanding face challenges.

Q39: Do you have thorough diagrams of the entire network including Wi-Fi?

A: No, thorough network diagrams vary.

Q40: Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?

A: No, FIM of critical data varies.