Executive Summary of Newstar Auto Digital Transformation – Capstone Project

Prepared By Pooya Molai

Introduction

Overview of Project: This presentation summarizes the comprehensive security and continuity measures developed to support Newstar Auto's digital transformation.

Key Deliverables: Cybersecurity Risk Assessment, Threat Modeling, Network and Data Security, Third-Party Risk, Incident Response Plan, and Business Continuity Plan.

Cybersecurity Risk Assessment

Core Processes Analyzed: Sales Process and Service Scheduling & Loyalty Program Management.

Key Risks: Lack of encryption, fragmented customer records, weak access controls.

Recommendations: Adopt a cloud-based CRM (Salesforce), implement role-based access control, and encrypt sensitive data both in transit and at rest.

Threat Modeling (STRIDE)

Key Components: Salesforce CRM, Cloud Storage, Service Department Devices, Network Infrastructure.

Identified Threats: Spoofing, Tampering, Information Disclosure, Denial of Service, Elevation of Privilege.

Mitigations: Strong authentication, data encryption, network segmentation, and monitoring.

Network and Data Security

Network Topology: Corporate and dealership networks connected to cloud services, secure VPN access for remote users, partner integration via API.

Identified Vulnerabilities: Firewall misconfigurations, outdated VPN protocols, insecure endpoint devices.

Mitigation Strategies: Upgrade VPN protocols, conduct firewall rule reviews, segment internal networks, implement endpoint security.

Third-Party Risk Management

Key Vendors: Salesforce CRM, Third-Party Scheduling System, Cloud Storage Provider, Partner Businesses.

Risks: Data breaches due to misconfiguration, third-party service outages, insecure API connections.

Shared Responsibility Model: Defined responsibilities for Newstar Auto and vendors regarding infrastructure security, access management, and data protection.

Mitigations: Strong SLAs, API security measures, continuous vendor monitoring.

Incident Response Plan

NIST Framework Phases: Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Post-Incident Activity.

Key Tools: SIEM, IDS/IPS, EDR, backup solutions.

Goals: Minimize impact of incidents, ensure timely detection, contain threats, recover systems quickly.

Communication Plan: Internal communication with the Crisis Management Team, external notifications to regulatory authorities and customers if needed.

Business Continuity Plan

Risk Assessment: Cyberattacks, natural disasters, system failures, third-party dependencies.

Continuity Strategies: Data backups, disaster recovery sites, remote work capabilities, crisis management team.

Recovery Plan: Restore critical systems, verify data integrity, communicate progress to stakeholders.

Customer and Employee Communication: Use secure channels to keep customers and staff informed during disruptions.

Summary of Recommendations

Data Protection: Implement encryption, RBAC, strong access controls.

Resilience: Establish disaster recovery capabilities, redundancy, and remote work infrastructure.

Vendor Management: Strengthen SLAs, monitor third-party risks, and define shared responsibilities clearly.

Incident Readiness: Train staff, conduct tabletop exercises, and update response plans regularly.

Conclusion and Next Steps

Conclusion: Newstar Auto's digital transformation offers significant opportunities but also introduces cybersecurity challenges. By following the outlined recommendations, Newstar Auto can ensure data security, operational continuity, and compliance with regulations.

Next Steps: Implement identified measures, train staff, collaborate with third-party vendors, and establish regular reviews of security policies.