Task ‘Disaster Recovery Plan Development’ Unit 9

Introduction

Businesses today rely on uninterrupted services. ABC-Europe-Logistics is a logistics provider vital to daily operations, the economy, and public safety. It is therefore classified as critical infrastructure. This report outlines the main risks facing ABC-Europe-Logistics and recommends developing a DRP report to improve resilience, service continuity and ensure compliance.

Identified Risks and Their Potential Impact

ABC-Europe-Logistics is a European logistics provider that relies heavily on cloud-based services to deliver its services. The company outsourced their IT and cloud service delivery to a Managed Service Provider (MSP). The organization is facing risks from possible cyberattacks, deficiencies in IT and IT-Security architecture, cloud services outages, and infrastructure failures on the MSP data center. These events could have a negative impact on confidentiality, integrity, availability and reputation on the organization.

(Deelstra, Bristow, 2023)

- **Cyberattacks**: A lack of detection capability on-premises and on the cloud, means that events may indicate incidents, which cannot be confirmed. This increases the risk of attackers going undetected.

- **IT and IT-Security Architecture Deficiencies**: Lack of patch encryption, outdated access controls, services, excessive and misconfigured firewall rules, and inconsistent enforcement of Multi-Factor Authentication (MFA) increase the risk of exposure to breaches.

- **Service Gaps**: The MSP's services have not aligned with industry best practices. Absence of Service Level Agreements (SLAs) and poorly defined contracts could negatively impact on performance, security, and accountability.

- **Operational Disruption**: In the event of a failure in the MSP data center or an outage of one of the dedicated connections to the cloud for instance AWS Direct Connect, this would cause a significant outage. The absence of asset management and security event monitoring hinders the capacity to restore service availability in a timely manner.

(Malka, A, 2025).

Service improvements

- Defined with MSP clear and effective and improved SLA's and contracts.

Monitoring and Continuous Improvement

- Deploy SIEM that collects data from centralized logging of all systems in hybrid environments including cloud including CASB integration.
- Maintain asset inventory and vulnerability scanning systems and perform scans on a regular basis.

Incident Response and Restoration capabilities

- Develop incident response based on ISO/IEC 27035, or another applicable framework.
- Develop threat hunting capabilities with IOC's, KRI, and incident response roles and responsibilities.
- Isolate affected systems when a true positive is detected.
- Restore services, use clean backups and images with checksum and hashing algorithms for integrity verification.
- Perform root cause analysis, post-Incident and apply lessons learned.

Operational Continuity

- Set Recovery Objectives RTO and RPO based on critical business functions.
- Establish communication protocols for internal teams, customers, and authorities.
- Conduct regular disaster recovery testing and audits.

Backup and Recovery Tools

- Deploy AWS Elastic Disaster Recovery to replicate cloud environments and ensure rapid recovery during outages.
- Use Bacula for automated, encrypted backups across.

IT and IT-Security Architecture Deficiencies

- Enforce MFA across all systems.
- Implement modern firewalls with real-time threat detection and effective configuration, for instance Implicit deny.
- Introduce full-disk encryption to secure data.

Reflection on Legal, Ethical, and Professional Considerations in implementing the DRP

ABC-Europe-Logistics is obligated to comply with all relevant European regulations when implementing the DRP, including GDPR, NIS2, and BSI, as well as in all locations where it operates. Local laws instruct companies to notify the relevant authorities of data breaches. The absence of response procedures and monitoring capabilities engenders compliance and reputational risks. ABC-Europe-Logistics must align its SLAs with its MSP. IT governance that is ethical includes protecting customer data, securing infrastructure and ensuring that recovery strategies are in place to ensure transparent and compliant business continuity and profitability.

References

Deelstra, A. and Bristow, D.N., (2023). Assessing the effectiveness of disaster risk reduction strategies on the regional recovery of critical infrastructure systems. Resilient Cities and Structures, 2(3), pp.41-52.

Malka, A, (2025). Security Risk Assessment Report: Security Measures to Mitigate Risks Unit 7 Available at: https://www.my-course.co.uk/mod/assign/view.php?id=1218399 [Accessed 15 September. 2025]

This document has been written solely for educational purposes. All references, names, and trademarks mentioned here remain the property of their respective owners and are used here strictly for the educational context. Grammarly was used exclusively for proofreading and enhancing the clarity and language of the text. All academic writing, analysis, argumentation, and conclusions are entirely the original work of the author.