Project Part 2

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

August 11, 2024

Business Continuity

Introduction

This business continuity plan addresses a scenario where a catastrophic event caused a major outage at the data center. This plan aims to minimize downtime and data loss, as well as ensure the continuity of critical business operations.

Business Impact Analysis

Critical Application and Data

- E-commerce Platform: handles all online sales and customer interactions. Impact revenue and company reputation.
- CRM System: stores sensitive customer data and manages customer relationships. Used for business operations and customer trust with the company's reputation.
- Proprietary Research Database: contains valuable intellectual property related to the company's research efforts. Required for research and development.

Impact of Outage
Qualitative Analysis

Qualitative Questions	2 hours	4 hours	8 hours	24 hours	48 hours	1 week
How will your clients react to a disruption?	2	2	3	3	3	4
What will be the impact to other activities?	1	2	2	3	3	4
How will the disruption influence the loss of reputation?	1	2	2	3	4	4

How difficult will it be to catch up on the backlog of work?	1	1	2	2	3	3

Quantitative Analysis

Quantitative Questions (in U.S. dollars)	2 hours	4 hours	8 hours	24 hours	48 hours	1 week
How much will the legal and contractual penalties cost?	$50,000	$100,000	$200,000	$500,000	$1,000,000	$5,000,000
How much will repair expenses be?	$10,000	$20,000	$50,000	$200,000	$300,000	$500,000
How much revenue will we lose?	$2.28 million	$4.56 million	$9.12 million	$27.4 million	$54.8 million	$191.8 million

Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO)

- MTPD: The maximum period that XYZ Corporation can withstand is 24 hours.
- Recovery Time Objective (RTO): the target time to restore normal operation is 8 hours.
    - E-commerce Platform: (minimal sales transaction losses)
    - CRM System: (customer data and business relationships)
    - Proprietary Research Database: (Protect valuable intellectual property)

Determining the RPO

	2 hours	4 hours	8 hours	24 hours	48 hours	1 week
E-commerce platform	1	2	2	3	3	4
CRM System	1	2	2	3	4	4
Proprietary Research Database	1	1	1	2	2	3

Recovery Strategies

Data Backup and Recovery

- Encryption on data backup to protect the data in transit and storage.
- Data Replication: to the second data center or partial cloud to ensure the RPO is met.
- Regular Backups: snapshots every 15 minutes and full backups at night stored offsite or in the hybrid cloud.

Redundant Systems

- Secondary Data Center
- HybridCloud

Failover

- Automatic Failover: the system should failover to the secondary data center or hybrid cloud.
- Load Balancing: to distribute traffic to balance the workload across multiple servers and data centers.

Communication Plan

- Management team: responsible for response and communicating with stakeholders.
- Stakeholder Communication: ensure communication in case of an outage.

Implementation Plan

Preparation

- Training: employees on business continuity procedures based on roles.
- Resource Inventory: ensure the inventory list is up to date of all critical assets.

Response

- Active Failover: Instant Failover.
- Data Recovery: Restore data.
- Communication: inform stakeholders.

Recovery and Restoration

- System Restoration: Restore the original data center.
- Testing test the restored systems.
- Post-Incident Review: identify improvements.

Test and Maintenance

Regular Testing

- Disaster Recovery Drills: test the BPC
- Plan Updates: updated the BPC to address new potential threats.

Continuous Improvement

- Feedback Mechanism: Get feedback on the incidents to improve.
- Ongoing Training: Keep employees trained about the procedures based on their roles for the BPC

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISCO. (n.d.). *Networking, Cloud, and Cybersecurity Solutions*. Cisco. https://www.cisco.com/site/ca/en/index.html

CrowdStrike. (n.d.). *The CrowdStrike Falcon® platform*. Crowdstrike.com. https://www.crowdstrike.com/platform/

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. https://www.fortinet.com/products/next-generation-firewall

ISO. (2023). *ISO/IEC 27001:2022(en)*. Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Lenaerts-Bergmans, B. (2021, December 8). *What is a Supply Chain Attack? | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

NIST. (2020). Security and privacy controls for information systems and organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

paloalto networks. (n.d.). *Global Cybersecurity Leader - Palo Alto Networks*. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/

rockwell. (n.d.). *MES Solutions for Life Sciences | FactoryTalk | US*. Rockwell Automation. Retrieved July 25, 2024, from https://www.rockwellautomation.com/en-ca/products/software/factorytalk/operationsuite/mes/life-sciences.html

SAP. (n.d.). *MES: The Power of Real-Time Data*. SAP. https://www.sap.com/canada/products/scm/execution-mes/what-is-mes.html

SOLARWINDS. (n.d.). *What Is WSUS? Windows Server Update Services Guide - IT Glossary | SolarWinds*. Www.solarwinds.com. https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services