1. Enumerate the potential risks to the quality and supply chain for the company **(Knowledge and Understanding weighted at 10%, Use of relevant sources weighted at 10%)**. This should include:
   1. The selection of quantitative risk modelling approach(es) with justification for the method chosen.
   2. Explanation of the calculations carried out, including detailed lists of assumptions and sources of data selected (where appropriate).
   3. Results of the quantitative models used.

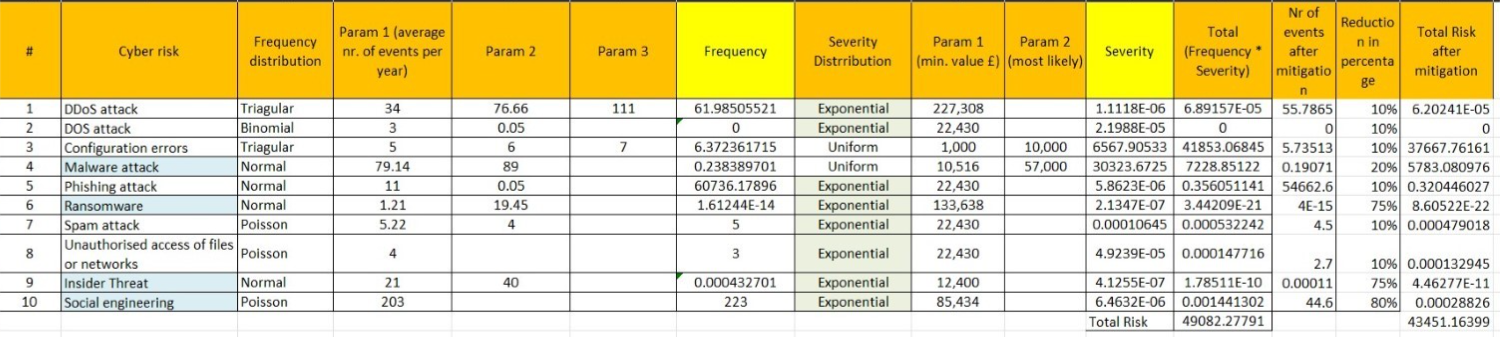
|  |  |
| --- | --- |
| Risks | Threats associated with the risks |
| Third party vendor risks | Data breach, third-party software attacks, malware and application installers |
| Digital risks | Zero-day exploits, overlooked configuration errors, ransomware, malware infection and non-compliance with regulatory standards |
| Supplier fraud | Social engineering attacks, phishing, AI generated voicemails and fake video recordings |
| Data Protection | Malware, ransomware, phishing and social engineering attacks (Edward, 2023) |

Table 1 - Supply Chain Risks

In the businesses with uncertainty of the risks, Monte Carlo risk modelling technique has always proved to be beneficial as per different research and since the business involves risks that are based on assumptions, using Monte Carlo risk modelling technique would help in the following ways.

* Answer the ‘what if’ scenarios and uncertainty of the different risks associated with the business.
* Helps to quantify the risks.
* The Monte Carlo technique would help the investors to decide on the full range of possible outcomes that can happen and compare it based on the various risk tolerance levels.
* The technique helps create a picture of the risk by using the probability distribution method. (Robert, 2021)

Results after Monte Carlo Simulation



Populating data table for Monte carlo table:

Social engineering attacks:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk type** | **Occurrence / year** | | **Occ / year (day)** | | | **Estimated cost of risk / year (UK)** | **Distribution (for MCS)** |
| **Min.** | **Max.** | **Average** | **Every x days** | **%**  **(x / 365)** |
| Social engineering | 203  attacks / year |  |  |  |  | £85,434 | Poisson |

1. Ms O’dour has also recommended that if the business is to be digitalised, there should also be put into place a business continuity/ disaster recovery (DR) strategy that will ensure that the business’ online presence could continue in the event of a disaster affecting the shop premises. The online shop needs to be available 24/7/365 with a less than 1 minute changeover window should DR need to be invoked. She has also recommended that the business cannot afford to lose more than 1 minute of data. Your team are tasked with the job of designing a DR solution that meets Ms. O’dour’s requirements. She also wants you to recommend the platform that should be chosen to host the solution and to provide advice on vendor lock-in. **(Knowledge and Understanding weighted at 10%, Criticality weighted at 10%, Use of relevant sources weighted at 5%)**.

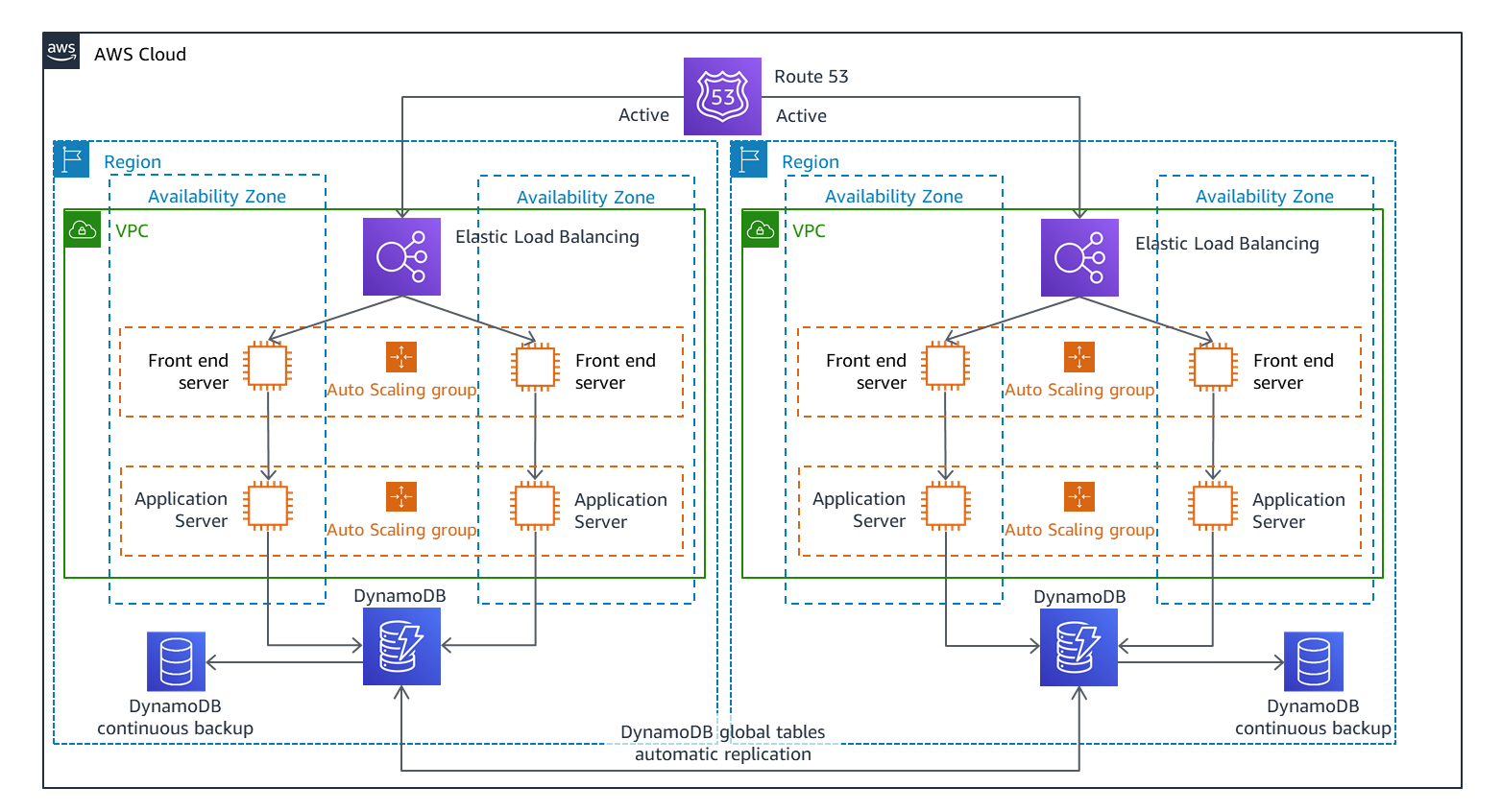
Plan for disaster Recovery:

* Saving documents and images in cloud platform example Amazon, Microsoft Azure or google cloud etc.
* Having an off-site backup (multi-regional backups).
* Data encryption of local hard drives.
* Keeping the network, system administrator and other members of the staff updated about the disaster recovery plan.
* Testing of the backup and recovery procedures.
* Secure data integrity and retention (Warith, 2022)

Platforms:

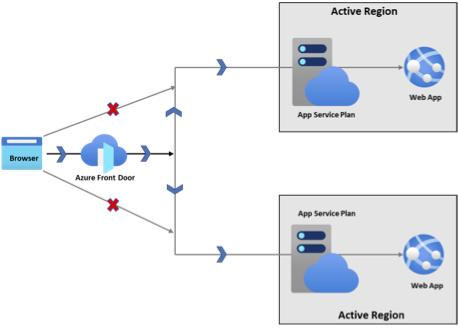
Amazon: multi-site active/active by Amazon

Amazon multi-site active/active strategy offers two or more regional sites for accepting requests in case of a failure. The requests are re-routed to the non-impacted regions which will keep the services running together with data backup in case of data deletion or corruption. However, it costs a lot of money in return for greatly reducing the RTO and RPO. (Seth, 2021)



Azure: active/active architecture by Azure

Microsoft Azure has a similar disaster recovery architecture which offers seconds of RTO and RPO. Azure active active architecture works by creating a front door that routes the traffic in both active regions. In case of disaster, the front routes the traffic to the active region hence giving an RTO of zero seconds. Like Amazon, the cost of the architecture is high as per the services offered.



**6. Security standards and mitigation for the business**

The security standards for Pampered Pets are based on the CIA-triad (Confidentiality, Integrity and Availability). The following security standards are recommended in order of business priority:

1. General Data Protection Regulation (GDPR) serves as the most crucial standard in protecting the service user’s rights and serves as a guide for the business to protect the personal information of the customer residing in the UK/EU.

2. Privacy policies and terms of service ensure that the data collected, stored, used and protected are clearly communicated with the service user.

3. Payment Card Industry Data Security Standards (PCI-DSS) ensure compliance with the payment methods.

4. Transport Layer Security/Secure Sockets Layer/Hypertext Transfer Protocol Secure (TLS, SSL, HTTPS) certificates provide service users with website safety verification and assurance.

5. Multi-Factor Authentication (MFA) implementation protects from unauthorised access.

The mitigations required to meet these standards revolve around implementing the above standards, strong passwords, timely updating and patching the system, employee training and awareness, incident response and management, and regular auditing (Arno, 2022).

References

Edward, K. (2023). The Biggest Security Risks in Your Supply Chain in 2023. Available from: https://www.upguard.com/blog/biggest-supply-chain-security-risks [Accessed 24 April 2023].

Robert, S. (2021). [Using Monte Carlo Analysis to Estimate Risk.](https://www.investopedia.com/articles/financial-theory/08/monte-carlo-multivariate-model.asp) Available from: https://www.investopedia.com/articles/financial-theory/08/monte-carlo-multivariate-model.asp [Accessed 24 April 2023].

Warith, N. (2022). Disaster Recovery Strategies To Keep Online Businesses Up And Running. Available from: https://www.forbes.com/sites/forbestechcouncil/2022/01/20/disaster-recovery-strategies-to-keep-online-businesses-up-and-running/?sh=5c6076992283 [Accessed 24 April 2023].

Seth, E. (2021). Disaster Recovery (DR) Architecture on AWS, Part I: Strategies for Recovery in the Cloud. Available from: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/ [Accessed 24 April 2023].

Cephaline and Onadebi (2023). Strategies For Business Continuity And Disaster Recovery In Azure App Service. Available from: https://learn.microsoft.com/en-us/azure/app-service/overview-disaster-recovery [Accessed 24 April 2023].

Statista (2023e) Number of cyber attacks reported to the Italian CERT (Computer Emergency Response Team) from 2018 to 2021, by attack method. Available from: <https://www.statista.com/statistics/649297/cyberattacks-distribution-share-by-method-in-italy-timeline/> [Accessed 18 May 2023].

Statista (2023f) Average costs of cyber insurance claims made by SMEs in North America from 2014 to 2018, by cause of loss. available from: <https://www.statista.com/statistics/667597/cyber-insurance-claim-cost-north-america-by-cause-of-loss/> [Accessed 18 May 2023].

# Arno, H (2022). E-commerce Security 101: Essential Information For Web Store Owners. Available from: https://www.sana-commerce.com/blog/ecommerce-security-101/ [Accessed 19 May 2022].

