**1.The risk assessment in duolingo.**

**1.1Physical threats**

Duolingo store the data of users and lessons. The physical threats from physics like earth quake, hurricane may destroy the hardware storing the data and damage the data. This can leads to the long-time disconnection of Duolingo service, the lost of user data and the lesson data, which will significantly reduce the user stickness, and the reliability of Duolingo. Furthermore, Duolingo may face the increasing costs of redesigning the course, rebuild the data storage infrastructure and the potential lawsuits from users.

for example, the Strasbourg Fire in 2021 made 2 data centers of OVHcloud badly damaged, which leaded to the disconnection of websites for about 3.6 millions and the lost of data. As a result, OVHcloud was subject to compensation claims exceeding €10 million and subsequently invested €30 million to rebuild the data center.

(<https://www.computerweekly.com/news/252520844/OVHCloud-facing-client-compensation-class-action-claim-of-10m-over-March-2021-datacentre-fire>)

**1.2 Electronic threats**

Duolingo is popular in the world especially as a e-learning platform of learing other languages, so it faces a huge number of electronic threats. The threats include hacking, phishing, data scraping through API, and also some malicious attacks like ddos, which may cause the data breach and damage the user rights, and ultimately reduce economic effciency.

In 2023, a public API from Duolingo is attacked by hackers, causing 2.6 million user data scraped, which decline the trust from user, leading to the loss of user, and increasing the cost to repair the API’s problem.

**1.3 Technical Failures**

Duolingo’s platform consists of a huge number of complex service, machine learning models and a lot of services. Once there are techincal problems in any of the process, it will lead to the failure of the whole system, and user may not be able to use some function of Duolingo.

“Duolingo Unexpected Application Error” is a common problems of using Duolingo, which may occur due to server problems or the problems related to the application itself.

(<https://duolingoguides.com/duolingo-unexpected-application-error/#google_vignette>)

**1.4 Infrastructure Failures**

Duolingo relays on the infrastructure to store the data, and make the data available for any region in the world. Poor infrastructure design or building may result in reduced availability and even data loss in Duolingo, affecting service continuity and risking irreversible loss to data.

Duolingo has experienced the infrastructure failure. On December 7, 2021, the AWS network outage caused Duolingo to go offline for 5 hours.

(<https://www.linkedin.com/pulse/why-devops-matters-duolingo-brad-plunkett>)

**1.5 Human Error**

Duolingo is delveoped by human, so the mistakes staff made can also be the risk of Duolingo. Mistakes can occur in strategy and techincal implementations. The strategy error means that the high-level mistaks in planning and direction, such as misidentifying the user’s requirements or ignoring the testing after developing. The human error may introduce significant risks to system security and stability.

The API problems in 1.2 also can be seen as the human error. In this case, the API can get the information from user through user name and user email, lacking of necessary access control and authentication mechanisms. It can be said that the data breach is originally due to human error.

**2. Security Best Practices: Research security strategies for similar organizations.**

The area focus on different e-platform security strategies.

**2.1 Canvas**

Canvas implements several strategies to prevent risks.

**Data Encryption**: All data in transit is encrypted using TLS 1.2 or higher, and data at rest is secured with AES-GCM 256-bit encryption. (<https://iser.mpc.edu/Standard-IIIC_Evidence_Folder/IIIC3-05_CanvasParticAgr.pdf>)

**Access Controls**: Canvas utilizes robust authentication and authorization mechanisms, including two-factor authentication (2FA), to ensure that only authorized users can access the platform. ​

**Regular Security Audits**: Instructure conducts continuous security assessments and adheres to industry standards such as SOC 2 and ISO 27001 to maintain a secure environment. ​(<https://www.instructure.com/trust-center>)

**Application Security**: All code undergoes peer review and automated security scans before deployment. Instructure also maintains a vulnerability disclosure program to engage the security research community.

**Content Security Policy (CSP)**: Administrators can manage CSP settings to restrict custom JavaScript execution, enhancing protection against cross-site scripting (XSS) attacks. ​(<https://community.canvaslms.com/t5/Admin-Guide/How-do-I-manage-the-Content-Security-Policy-for-an-account/ta-p/149>)

**2.2 Moodle**

**Regular software updates** are essential for addressing known security flaws. By keeping the Moodle core system and its plugins up to date, administrators ensure that vulnerabilities identified in previous versions are patched, reducing the risk of exploitation.

S**trong password policies**. These include minimum complexity requirements and optional multi-factor authentication, making it harder for attackers to succeed through brute-force or credential-stuffing attacks.

**Role-based access control (RBAC)** further enhances data protection by ensuring users only have access to the information and tools relevant to their roles. This principle of least privilege minimizes the chance of data being exposed due to over-permissioned accounts.

**Encryption protocols** such as SSL/TLS are used to protect information during transmission. This prevents sensitive user data—like login credentials or grades—from being intercepted in transit.

R**egular data backups**, allowing the system to be quickly restored in the event of hardware failure, accidental deletion, or cyber incidents such as ransomware attacks.

A**nti-malware and antivirus tools** into the hosting environment helps scan for and remove malicious software, ensuring system integrity.

**Activity logging and user monitoring** are implemented to track system usage and detect suspicious behavior. This allows for faster response to anomalies and potential breaches.

**3. Cybersecurity Threats: Discuss potential threats and compliance risks.**

Duolingo must also address emerging cybersecurity threats driven by rapid technological development, while ensuring compliance with data protection laws across different regions.

**3.1 Potential Threats**

With the deveoping of AI technology, there the attack methods can be variety.

**Prompt Injection:** Attackers use the special prompt, make the AI model in duolingo generating or leaking the user data.

**GANs for phishing :** Attacker use the GANs to create fake websites, tricking user inputing real information.

**AI-assisted password cracking**: Attackers use AI to predict and crack passwords more efficiently, allowing them to gain unauthorized access to user accounts and personal data.

**AI-powered malware development:** Attackers used AI to write complex, adaptive malicious code that traditional antivirus detection can not prevent.

**3.2 Compliance risks**

In different region, there are different laws for protecting the data, as a global e-learning platform, Duolingo need to make sure that the application is statisfy the compliance.

For example, **GDPR**(General Data Protection Regulation) is a regulation in Europe, containing the right of user, the security about user data, the strategy need to take after data leakage, which will lead to over 20 millions Euros fine. **CCPA**(California Consumer Privacy Act) stipulates that the user should have the right to know the data Duolingo collecting from them and can ask Duolingo to delete their data.

Duolingo needs to follow the regulations in different countries and area, to prevent from the potential economic losses.