Coursework

Comp1843: Principles of Security

University of Greenwich ID Number: 001366556

FPT Student ID Number: GCH230330

Student's name: Nguyen Duy Tan

Course: COMP-1843

Lecturer Name: Michael Omar

Table of Contents

List of Tables

1. Management Summary

DiGi is a tech start-up specializing in dynamic and interactive software development, with a focus on integrating its products with various platforms such as Android and Apple. With a customer base that spans from small and medium-sized enterprises (SMEs) to larger industry players, DiGi has gained considerable traction in the market. The recent crowdfunding of £8.4 million has provided the company with the necessary capital to expand its operations globally.

However, this expansion presents several risks, particularly in the areas of cybersecurity, system scalability, and legal compliance. The existing infrastructure, which has served DiGi well so far, may struggle to cope with the increased demands, potentially leading to system failures or security breaches. Additionally, the flat organizational structure of the company, while fostering innovation and flexibility, has created challenges in role clarity and data management.

This report provides a comprehensive risk assessment, identifying the key vulnerabilities and threats facing DiGi. The report also evaluates the company's critical assets using a weighted factor analysis and creates a risk register prioritizing these risks based on their probability and impact. Finally, the report proposes strategic risk control measures to mitigate these risks, ensuring that DiGi can achieve sustainable growth while maintaining high standards of security, compliance, and operational efficiency.

By implementing the recommended strategies, DiGi can not only protect its existing assets and operations but also position itself as a leader in the competitive tech industry, ready to meet the challenges of future growth

2. Risk identification

2.1. Risk Identification Process

2.1.1. Identify, Inventory, & Categorize Assets

DiGi's assets encompass both tangible and intangible items crucial to its operations. These include physical hardware, proprietary software, customer data, intellectual property, and human resources. The table below categorizes these assets:

Table 1: Asset Identification and Categorization

Asset	Category	Description
Customer Data	Data	Personal and payment information of customers
Proprietary Software	Intellectual Property	DiGi’s developed software applications
Employee Workstations	Hardware	Computers and devices used by employees
Development Tools	Software	Licensed tools for software development
Brand Reputation	Intangible	Market perception and brand value

2.1.2. Classify, Value, & Prioritize Assets To assess the significance of each asset, they are classified and prioritized based on their value to DiGi. High-value assets are those that are critical to business continuity, such as customer data and proprietary software.

Table 2: Asset Classification, Valuation, and Prioritization

Asset	**Classification**	**Valuation**	**Priority**
Customer Data	Critical	High	1
Proprietary Software	Critical	High	2
Brand Reputation	Strategic	High	3
Employee Workstations	Operational	Medium	4
Development Tools	Operational	Medium	5

2.1.3. Identify & Prioritize Threats

Identifying potential threats that could exploit vulnerabilities in these assets is essential. These threats may include both external and internal factors.

Table 3: Threat Identification and Prioritization

Threat	**Description**	**Likelihood**	**Impact**	**Priority**
Cyber Attacks	Phishing, malware, ransomware	High	High	1
Data Breaches	Unauthorized access to customer data	Medium	High	2
Intellectual Property Theft	Stealing proprietary software	Medium	High	3
Insider Threats	Malicious actions by disgruntled employees	Low	Medium	4
Legal Compliance Issues	Failure to meet regulatory requirements	Medium	High	5

2.1.4. Specify Asset Vulnerabilities

Vulnerabilities in DiGi's assets can be exploited by the identified threats. These vulnerabilities must be clearly specified to understand the level of risk associated with each asset.

Table 4: Asset Vulnerabilities

Asset	**Vulnerability**	**Associated Threat**	**Severity**
Customer Data	Weak encryption protocols	Data Breaches	High
Proprietary Software	Inadequate intellectual property protection	Intellectual Property Theft	High
Brand Reputation	Lack of crisis management plan	Cyber Attacks, Data Breaches	Medium
Employee Workstations	Outdated security software	Cyber Attacks, Insider Threats	Medium
Development Tools	License management issues	Legal Compliance Issues	Low

2.2. Analyze Vulnerabilities

2.2.1. Organization-Specific Vulnerabilities (Based on Assumptions)

Given DiGi's start-up status, specific vulnerabilities may include a lack of established security protocols, limited cybersecurity expertise, and an overreliance on third-party tools that may not meet rigorous security standards.

2.2.2. Impact of Vulnerabilities on Critical Assets

Vulnerabilities in critical assets, such as customer data and proprietary software, could have severe consequences for DiGi, including financial losses, legal penalties, and damage to the company's reputation. Ensuring these assets are protected is crucial for the company's long-term success.

2.3. Predicting Threats

2.3.1. Potential Threats that DiGi May Encounter

DiGi may face a variety of threats, including cyber attacks (phishing, ransomware), data breaches, and insider threats, particularly as it scales operations and attracts more attention.

2.3.2. Current Security Trends of SMEs and Their Application to DiGi

Security trends for SMEs include increased reliance on cloud services, growing incidents of ransomware, and a shift towards more sophisticated phishing attacks. DiGi must be proactive in adopting security measures that align with these trends, such as robust encryption, regular security audits, and employee training programs.

3. Risk Management

3.1. Asset Identification and Evaluation

3.1.1. Use the Weighted Factor Analysis method to determine property determination

Table 5: Weighted Factor Analysis

Asset	**Weight (Importance)**	**Score**	**Weighted Score**	**Rationale for Score**
Customer Data	**30%**	**8/10**	**2.4**	**Critical for operations and customer trust.**
Intellectual Property (IP)	**25%**	**9/10**	**2.25**	**Core asset for DiGi, crucial to business growth and competitiveness.**
Financial Data	**20%**	**7/10**	**1.4**	**Essential for operational continuity but less exposed than IP and customer data.**
Employee Information	**15%**	**6/10**	**0.9**	**Important but lower risk than other assets due to limited external threats.**
Software Systems	**10%**	**8/10**	**0.8**	**Key to service delivery but more resilient to disruption than data assets.**

In this table, assets are evaluated based on their importance to the organization, with scores assigned for their criticality. The weighted score reflects the impact of each asset on overall operations.

- **3.1.2. Evaluation and ranking table of important assets**

Table 6: Asset Evaluation and Ranking

Asset	Rank	Justification
Intellectual Property (IP)	1	Most critical for business growth and competitive edge.
Customer Data	2	Vital for maintaining customer trust and regulatory compliance.
Financial Data	3	Essential for operational continuity, though less exposed.
Software Systems	4	Important for service delivery, but resilient with backups.
Employee Information	5	Lower risk, with fewer external threats compared to other assets.

This table ranks assets based on their criticality to the organization's success and the potential impact of their compromise.

3.2. Risk Register

- **3.2.1. List risks and priorities**

Table 7: Risk Register

Risk	Impact Level	Likelihood	Priority	Mitigation Strategy
Data Breach (Customer Data)	High	Medium	1	Enhanced encryption, regular audits.
IP Theft	Very High	High	2	Strict access control, legal protections.
Financial Fraud	High	Low	3	Strong financial controls, multi-factor authentication.
System Downtime	Medium	Medium	4	Backup systems, disaster recovery plans.
Employee Data Loss	Low	Low	5	Secure storage, limited access.

This table lists the risks identified for DiGi, prioritizing them based on their potential impact and likelihood. Each risk is paired with a corresponding mitigation strategy.

- **3.2.2. Analyze the reasons for ranking these risks**

The risks are ranked according to their potential impact on DiGi's operations and the likelihood of their occurrence. Data breaches and IP theft are prioritized due to their significant consequences for the company's reputation and competitive position. Financial fraud, while severe, is considered less likely due to existing controls. System downtime is a medium priority due to its impact on service delivery, and employee data loss is ranked lowest as it poses the least external risk to the organization.

4. Risk Control Strategies (20%)

4.1. Avoid Risks (Avoidance)

- **4.1.1. Measures to Eliminate or Reduce the Risk of Incontinence**

  To eliminate or reduce risks, DiGi can implement the following measures:

  - **Strict Access Controls:** Implement role-based access control (RBAC) to ensure that only authorized personnel have access to sensitive information, reducing the risk of data breaches.
  - **Regular Security Audits:** Conduct frequent audits to identify and rectify potential security vulnerabilities before they can be exploited.
  - **Employee Training:** Regular training sessions for employees on security best practices to minimize the risk of human error leading to security incidents.

4.2. Risk Transfer (Transference)

- **4.2.1. Risk Transfer Measures Such as Outsourcing and Insurance**

  DiGi can manage some risks by transferring them to third parties:

  - **Cybersecurity Insurance:** Purchase cybersecurity insurance to cover potential losses from data breaches, cyber-attacks, and other security incidents.
  - **Outsourcing to Specialized Security Firms:** Outsource the management of certain security operations, such as network monitoring and incident response, to specialized third-party providers with expertise in these areas.

4.3. Minimize Risks (Mitigation)

- **4.3.1. Measures to Minimize the Impact of Risks (DRP, IRP, BCP)**

  To mitigate the impact of risks that cannot be completely avoided or transferred, DiGi should consider:

  - **Disaster Recovery Plan (DRP):** Develop and regularly update a disaster recovery plan to ensure quick recovery of IT systems and data in the event of a major incident.
  - **Incident Response Plan (IRP):** Establish an incident response plan with clear procedures for detecting, responding to, and recovering from security incidents.
  - **Business Continuity Plan (BCP):** Create a business continuity plan to ensure that critical business functions can continue during and after a disaster, minimizing disruption to operations.

4.4. Accept Risks (Acceptance)

- **4.4.1. When to Take Risks and Not Take Measures to Prevent**

  In some cases, DiGi may decide to accept certain risks if the cost of mitigation exceeds the potential impact of the risk. This decision should be based on a careful analysis of the risk's likelihood and potential consequences. For example:

  - **Low Impact/Low Likelihood Risks:** DiGi might choose to accept risks that have a low likelihood of occurring and would not significantly impact the business if they did occur, rather than investing resources in mitigation strategies.

5. Conclusion

In this report, we conducted a comprehensive risk assessment for DiGi, a tech start-up poised for global expansion. As the company grows, it faces increasing risks, particularly in cybersecurity, system scalability, and legal compliance. Through a detailed risk identification process, we have highlighted the most critical assets, such as customer data and intellectual property, and identified potential threats including cyber-attacks, data breaches, and intellectual property theft.

Our risk management analysis utilized a weighted factor approach to prioritize these assets and associated risks, ensuring that the most significant threats are addressed first. We then proposed a series of risk control strategies, ranging from risk avoidance and transference to mitigation and acceptance. These strategies are designed to protect DiGi’s key assets and ensure operational continuity as the company scales.

By implementing these recommended strategies, DiGi can not only safeguard its current operations but also build a resilient foundation for future growth. This will enable the company to maintain its competitive edge, protect its reputation, and continue to innovate in the dynamic tech industry.

Ultimately, the proactive management of risks will be crucial to DiGi’s success, allowing it to navigate the challenges of expansion while upholding the highest standards of security and compliance.

6. References

1. Andress, J. (2014) *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd edn. Waltham, MA: Syngress.

2. Stallings, W. (2016) *Cryptography and Network Security: Principles and Practice*. 7th edn. Boston: Pearson.

3.Whitman, M.E. and Mattord, H.J. (2018) *Principles of Information Security*. 6th edn. Boston: Cengage Learning.

4. Gordon, L.A. and Loeb, M.P. (2002) 'The economics of information security investment', *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp. 438-457.

5. von Solms, R. and van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security*, 38, pp. 97-102.

6..Peltier, T.R. (2016) *Information Security Risk Analysis*. 3rd edn. Boca Raton, FL: Auerbach Publications.

7.NIST (2012) *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed: 15 August 2024).

8. ENISA (2020) 'Threat Landscape 2020'. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020 (Accessed: 15 August 2024).

9. ISACA (2019) *State of Cybersecurity 2019: Current Trends in Threats, Awareness, and Governance*. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/state-of-cybersecurity-2019 (Accessed: 15 August 2024).