TRANSPORTATION COMPANY

VIETPHAT

+123-456-7890 www.VietPhatTrans.com VietPhat@gmail.com

WELCOME TO OUR COMPANY

Company Overview:

- Name: Viet Phat Transportation Company
- Industry: Transportation and Logistics
- Established: 2005
- Headquarters: Ho Chi Minh City, Vietnam
- Key Services/Products: Freight transportation, fleet management, logistics solutions, and warehousing services

OUR SYSTEM

Customer Data Management System

- Functions: Storing and processing customer data, transaction history, and communication records.
- Users: Approximately 500 users, including employees and third-party vendors.
- Technology: Python, SQL, Django framework.
- Version: 3.2.1
- Hosting Environment: Cloud (AWS)
- Vulnerabilities: Insufficient data encryption, potential for unauthorized access.

Network Infrastructure Management System

- Functions: Managing and securing network infrastructure, including servers and routers.
- Users: Approximately 100 network administrators and IT staff.
- Technology: Java, Kubernetes, Docker.
- Version: 2.1.0
- Hosting Environment: Hybrid (Cloud and On-premises)
- Vulnerabilities: Exposure to DDoS attacks.

GPS Tracking Software

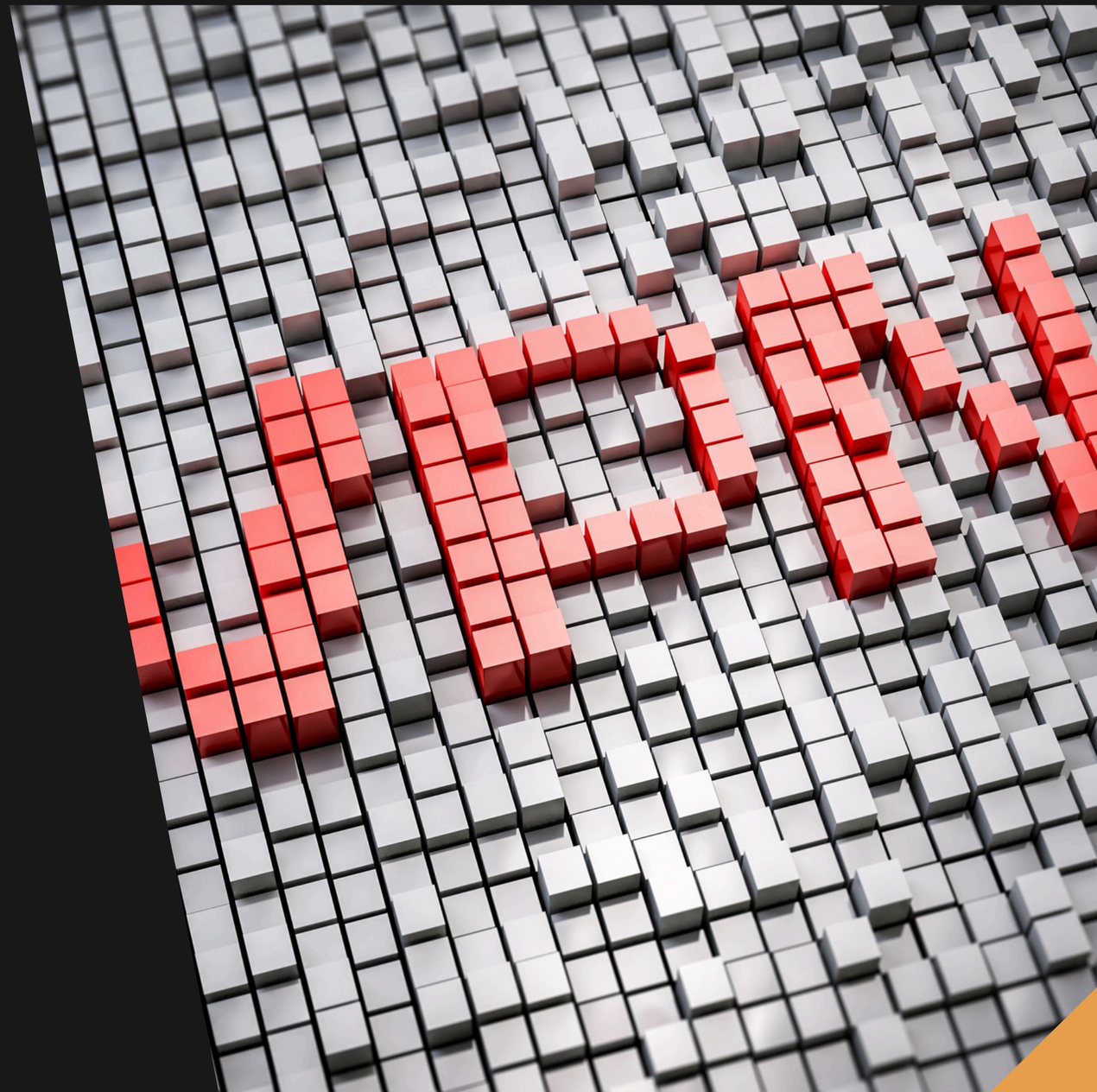
- Functions: Tracking fleet vehicles, managing logistics and route planning.
- Users: Approximately 200 users including operations and logistics staff.
- Technology: .NET, SQL Server.
- Version: 4.5.3
- Hosting Environment: On-premises
- Vulnerabilities: Software vulnerabilities, lack of regular updates.

Web Servers

- Functions: Hosting the company's web applications and online services.
- Users: Public-facing, accessed by customers and partners.
- Technology: Node.js, React, MongoDB.
- Version: 1.8.7
- Hosting Environment: Cloud (Azure)
- Vulnerabilities: Web server software vulnerabilities, risk of SQL injection.

VPN

- Functions: Secure remote access to the company network.
- Users: IT staff and remote employees.
- Technology: OpenVPN, IPSec.
- Version: 2.9.4
- Hosting Environment: On-premises
- Vulnerabilities: Reverse VPN



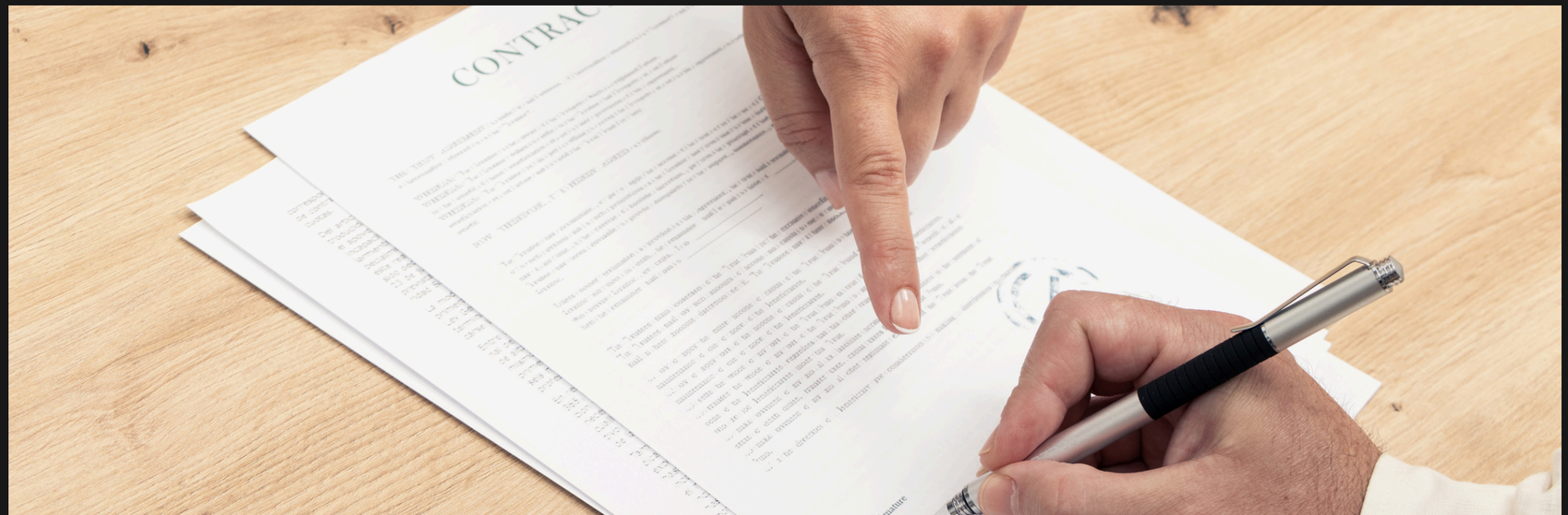
REGULATORY COMPLIANCE

01 GDPR: General Data Protection Regulation for data protection and privacy in the EU.

02 HIPAA: Health Insurance Portability and Accountability Act for healthcare data.

03 PCI DSS: Payment Card Industry Data Security Standard for payment processing.

04 SOX: Sarbanes-Oxley Act for financial reporting and auditing.



PAST INCIDENTS

01

System Downtime (July 2022): Outage caused by a DDoS attack, affecting service availability for 6 hours.

02

Data Breach (March 2023): Compromised customer data due to a phishing attack, affecting 10,000 customers.

03

Compliance Violation (December 2021): Non-compliance with GDPR, leading to a fine of $50,000.

SCOPE OF THE RISK ASSESSMENT PROJECT

Objective: To identify, assess, and mitigate risks associated with the Customer Data Management System, Network Infrastructure Management, GPS Tracking Software, Web Server, VPN Server .

Stakeholders:

- Internal: IT Department, Security Team, Compliance Team, Executive Management
- External: Third-party vendors, Regulatory bodies

ASSESSMENT AREAS

01

Asset Identification: Cataloging all assets within the system

- **Details**:
  - Customer databases
  - User access controls
  - Encryption keys
  - Backup systems

ASSESSMENT AREAS

02

Threat Analysis: Identifying potential threats

- **Details:**
  - Malware and ransomware
  - DDoS attacks

ASSESSMENT AREAS

03

Vulnerability Assessment: Evaluating weaknesses in the system

- **Details:**
  - Lack of data encryption
  - Insufficient user access controls
  - Outdated software versions
  - Misconfigured network service.

ASSESSMENT AREAS

04

Impact Analysis: Assessing the potential impact of different threats

- **Details:**
  - Data loss or corruption
  - Legal penalties
  - Financial losses

ASSESSMENT AREAS

05

Control Evaluation: Reviewing current controls and identifying gaps

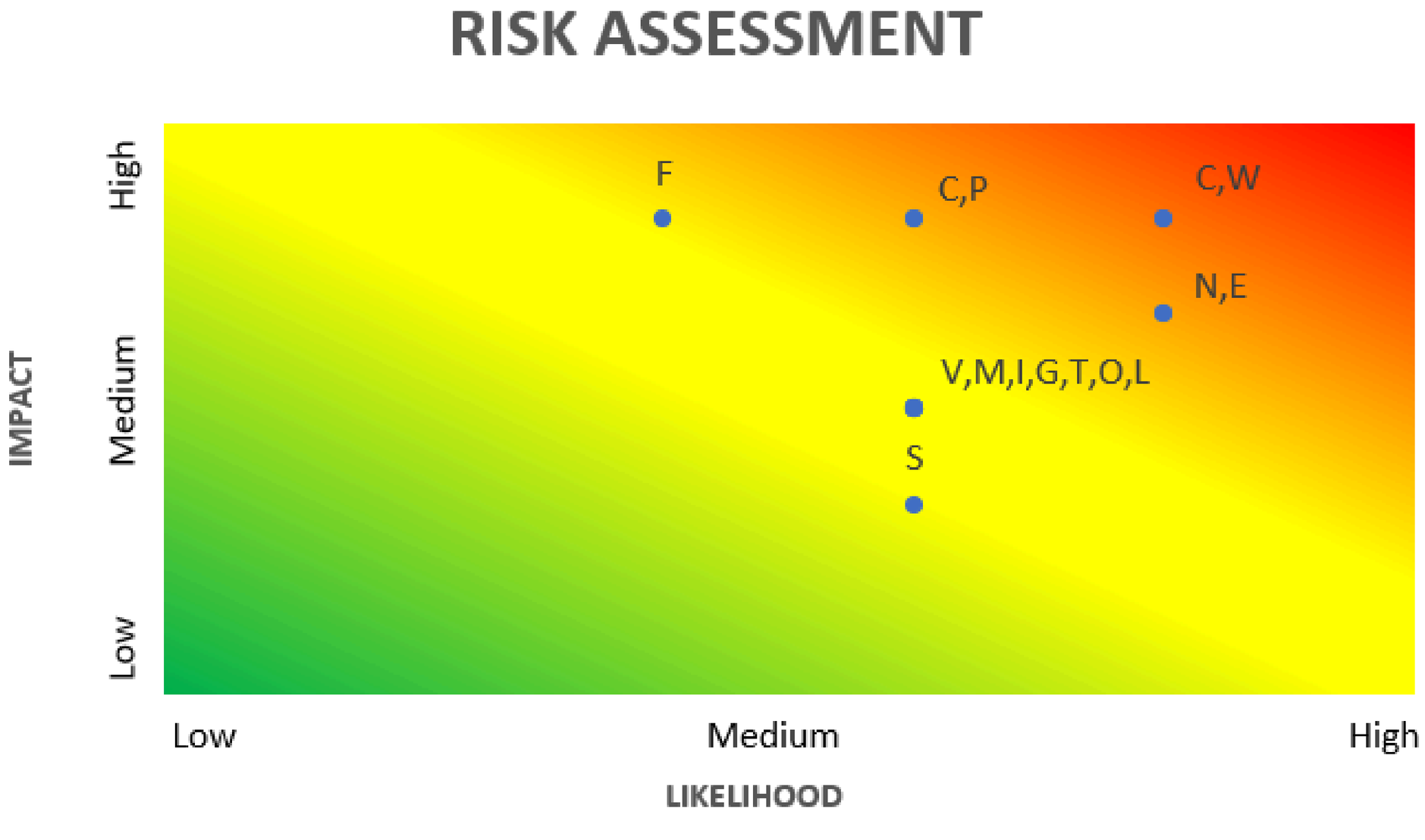
- **Details:**
  - Firewalls and intrusion detection systems
  - Regular software updates
  - Data backup procedures

RISK ASSESSMENT

Risk ID	Asset	Threat	Likelihood (1-5)	Impact (1-5)	Risk Level (1-25)
1	Customer Data	Data breach involving customer data	4	5	20
2	Network Infrastructure	DDoS attack on network infrastructure	4	4	16
3	GPS Tracking Software	GPS tracking software exploitation	3	3	9
4	Fleet Management Software	Unauthorized access to fleet management system	3	3	9
5	Web Servers	Security breach of web servers	4	5	20
6	VPN Gateways	VPN gateway compromise	3	3	9
7	Employee laptops	Theft or loss of laptops	3	3	9
8	Financial records	Financial fraud	2	5	10
9	Office workstations	Malware infection	3	3	9
10	Email servers	Email phishing attacks	4	4	16
11	Ticketing System	Attack on ticketing system	3	3	9
12	Cloud Services	Unauthorized access to cloud services	3	5	15
13	Social Media Accounts	Hacking of social media accounts	3	2	6
14	IoT Sensors	Unauthorized access to IoT sensors	3	3	9
15	Payment Processing Systems	Unauthorized access to payment processing systems, Fraud	3	5	15

HEATMAP

C	Customer Data
N	Network Infrastructure
G	GPS Tracking Software
M	Fleet Management Software
W	Web Servers
V	VPN Gateways
L	Employee laptops
F	Financial records
O	Office workstations
E	Email servers
T	Ticketing System
C	Cloud Services
S	Social Media Accounts
I	IoT Sensors
P	Payment Processing Systems



DETAILED RISK ASSESSMENT WITH IN-PLACE / PLANNED CONTROLS

Risk	In-Place Controls	Planned Controls
Data Breach Involving Customer Data	Encryption	Enhanced Intrusion Detection Systems (IDS)
	Multi-factor Authentication (MFA)	Regular Security Audits
DDoS Attack on Network Infrastructure	Redundant Systems	Implement measures to prevent and mitigate distributed
	Regular Backups	Improved Failover Mechanisms
GPS Tracking Software Exploitation	Secure API Integration	Conduct thorough code reviews to identify and fix security issues.
	Regular Security Assessments	Regularly update the software to patch vulnerabilities.
Unauthorized Access to Software of Company	Access Controls	Enhance access control with biometric verification.
	Network Segmentation	Regular Penetration Testing
Security Breach of Web Servers	Web Application Firewalls (WAF)	Encourage security researchers to report vulnerabilities.
	Regular Security Updates	Implement tools to detect and respond to threats in real-time.
VPN Gateway Compromise	Strong Encryption	Regular Security Audits
	MFA for VPN Access	VPN Gateway Upgrades
Theft or Loss of Laptops	Endpoint Security Software	Remote Wipe Capability
	Encryption	Employee Training
Financial Fraud	Encryption	Regular Audits
	Access Controls	Advanced Threat Protection
Malware Infection	Antivirus Software	User Training
	Email Filtering	Network Monitoring
Email Phishing Attacks	Spam Filters	Phishing Simulations
	User Training	Advanced Email Security Solutions
Attack on Ticketing System	Access Controls	Regularly apply security patches to the ticketing system.
	Regular Security Assessments	Train users on secure practices when using the ticketing system
Unauthorized Access to Cloud Services	Use strong encryption for data stored and processed in the cloud.	Regular Security Audits
	Define and enforce strict access controls for cloud services.	Implement tools to continuously monitor cloud compliance.
Hacking of Social Media Accounts	Strong Passwords	Review account access and activity regularly.
	Two-Factor Authentication (2FA)	Security Training
Unauthorized Access to IoT Sensors	Isolate IoT devices on a secure network	Advanced Threat Detection
	Regular Firmware Updates	Security Training
Unauthorized Access to Payment Processing Systems	Encryption	Fraud Detection Tools
	Access Controls	Regular Security Audits

THANK YOU