Cybersecurity Status Report

Prepared for:

Zenith Logistics Managing Directors

Prepared by:

Abir Hasan Shuvo

Information Systems Security Auditor

Submitted on:

11 April 2025

Executive Summary

Zenith Logistics—an Australian supply chain and logistics company that powers critical functions for retail, manufacturing, and e-commerce. As the organisation continues its exponential growth, cybersecurity risks are escalating from outdated infrastructure and unpatched legacy systems along with uncoordinated security practices in a hybrid IT environment.

This report provides a review of cybersecurity status using the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework. Using this approach, we determine Zenith's most sensitive information assets, such as the proprietary LogiFlow system, inventory management modules, and financial transaction networks. These systems face external threats like ransomware and unauthorized access, and internal vulnerabilities such as bad endpoint security and lack of user education.

Foremost among the discoveries were several security hollows encompassing authentication conventions, information taking care of methods, and outsider combinations. Risk exposure is increased due to a lack of structured incident response planning and inconsistent enforcement of policies.

In response to these challenges, this report discusses the importance of prioritizing the following mitigation strategies: implementation of multi-factor authentication, establishment of formal incident response procedures, enhancement of access controls and provision of organization-wide cybersecurity training.

By taking these steps, Zenith Logistics can minimize its threat surface substantially, bolster operational resilience, and bring its information security practices in line with the industry's highest standards—fuelling sustainable growth and long-term client faith in the firm.

Table of contents

Introduction

As your designated Information Systems Security Auditor, this cybersecurity status report provides an in-depth overview and assessment of the current cybersecurity posture of Zenith Logistics, using the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) risk assessment framework. OCTAVE is well-known for the systematic, strategic method for identifying, assessing and minimizing information risks and is particularly well-suited for complex environments like logistics and supply chain operations.

It helps identify and prioritise operationally critical information assets and their potential threats and vulnerabilities, assesses the likelihood and impact of these threats, and determines which risks have the largest impact on the potential business consequences. This report, in accordance with industry standards and best practices, also recommends appropriate mitigation strategies and internal controls to reduce exposure and enhance resilience.

This step is designed not just to protect Zenith's critical infrastructure, but also to help ensure that you can maintain business continuity, client trust and regulatory compliance. In the end, the idea is to provide a clear, actionable map to get you better cyber defensive whilst still aligning to business priority & strategic goals.

Strategic Context, Value-Creation, Risk Posture & Mission Statement

Strategic Environment & Value-Creation

Zenith Logistics is a national provider of supply chain and logistics services serving retail, manufacturing and e-commerce companies. Its operations span warehousing, inventory management, transportation, last-mile delivery and real-time tracking — all managed through its proprietary LogiFlow platform. The company has increased rapidly but still operates on old infrastructure, hybrid IT model and legacy components that were not originally built with modern cybersecurity in mind.

Current Cybersecurity Risk Posture

Zenith, at present, functions under a malleable risk posture the mark of which is inconsistent security enforcement, inept user training, and disjoined system updates. This has put key systems at risk of ransomware attacks, attempts at unauthorized access, and operational disruptions. Weak resilience is also due to a lack of centralized incident response planning and delayed cloud adoption.

Cybersecurity Advisory Mission Statement

Consequently, Zenith Logistics is dedicated to delivering secure, non-disruption logistics services for our clients by pre-emptively managing these cybersecurity risks with strategic controls across the organization. We guard customer, operational, and financial data as part of the mission of cybersecurity–enabling scalable, secure business growth.

We limit technology transitions induced by innovation to controlled and quantifiable risk and are therefore more conservative in our approach. But we have zero tolerance for data loss or unauthorized access, or for system downtime that could interfere with your operations or violate compliance obligations.

Our security may be our way of being consistent with our inner values — trust, reliability, efficiency — for every digital process and every employee action in our organization.

This diagram reflects the business alignment of Zenith Logistics' business, cybersecurity, and risk management principles. This visual framework shows how the organization’s cybersecurity mission aligns with operational and strategic decisions. It is a measure of Zenith's focus on responsible, scalable growth without extreme exposure to risk, and its strict zero-tolerance stance towards the loss of sensitive data or prolonged system downtime

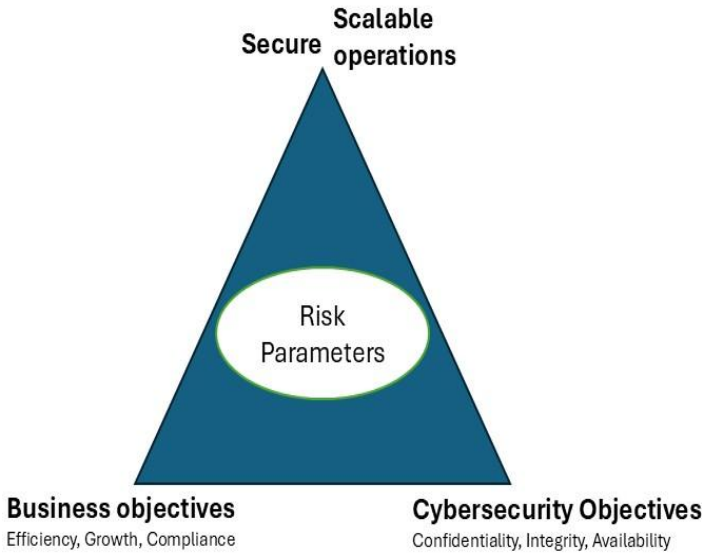

Figure 1: Strategic Alignment of Zenith's Cybersecurity Mission

Roles, Responsibilities, and Information Risk Assessment

An existing state of the cybersecurity framework of Zenith Logistics indicates a fragmented assignment of responsibilities across the technical, financial, and operational departments of the logistics provider. Though specific positions focus on information systems management, there is no centralized governance and not an effective integration between business units and IT security. This disconnect leads to weaknesses, missed obligations, and higher chances of data loss and outages.

These are the key roles and responsibilities, and an assessment of information risks and gaps:

Roles	Primary Responsibility	Oversees Information Assets	Risks/Gaps Identified
James Crawford & Rachel Liu (Managing Director)	Strategy and decision making	IT governance, IT policy, etc	Minimal engagement in cybersecurity matters; failure to focus on digital risk
Alex Grant (Security Team Lead)	Building and overseeing the cybersecurity framework	Network architecture, firewalls, endpoint security	couldn't realize comprehensive coverage across all systems
Liam Park (IT Security Analyst)	Monitoring systems, logging incidents, identifying threats	LogiFlow platform, endpoint devices, VPN access	Lacks authority to enforce policies or escalate changes; overwhelmed by system complexity
Ryan Cooper (Lead Software Developer)	Maintenance and patching of LogiFlow and integrations	Custom software, 3rd-party APIs, system logs	Integration vulnerabilities remain unpatched due to limited budget and compatibility issues
Mark Evans (CFO)	Financial oversight, IT investment decisions,	Financial systems, vendor management, cloud SaaS contracts	Not willing to fund cloud security upgrades
Sophia Bennett (Customer Relations Manager	Customer interaction and service technology quality	Customer orders data, tracking data,	CRM Orders vs shipment status mismatches; Needs more training in how to handle customer data securely.
Warehouse & Logistics Team	Daily operational data entry, inventory updates	Warehouse task	Management software Low cyber maturity and awareness, circumvent security [e.g., USB, weak passwords]

Full inventory of all information assets

A comprehensive audit of Zenith Logistics' information environment has identified key physical and logical assets used in logistics operations. The full inventory of these assets, including sensitivity levels and associated systems, is documented in **Appendix A at the end of this report.**

Asset, Threats, and Vulnerabilities Analysis (ATV)

A targeted analysis of Zenith Logistics' most critical information assets, utilizing the OCTAVE risk assessment method. The next table lists seven high-value operational assets, their major threats and associated vulnerabilities. These are chosen based on their effect on business continuity, data integrity, and regulation exposure.

Asset	Threats	Vulnerabilities
LogiFlow Database	Ransomware attack, data manipulation, unauthorized access	Legacy system with weak encryption, no MFA, unpatched modules
Inventory Management System	Phishing attacks, inaccurate stock data injection	Insufficient user training provided, insecure room devices, outdated access control
GPS Fleet Tracking System	Data spoofing, unauthorized vehicle tracking	Insecure IoT endpoints, no real-time alerting
Customer Profiles & Order Records	Identity theft, data breach	Shared login credentials, unencrypted storage, insufficient role-based access
Financial Transaction Logs	Fraudulent transactions, invoice tampering	Incomplete audit logs, poor third-party integration security
Supplier Coordination Portal	Supply chain disruption, information leakage	Weak partner authentication, no standard f API security

Employee Records & HR Systems	Internal data misuse, unauthorized payroll access	audit trails not available, improper entitlement, lack of user activity monitoring

Supporting Analysis and Explanation

1) All Logistics Operations are governed by the LogiFlow Database. The complexity with the treatment of patchy third-party extensions raises the attack surface to expose to ransomware (malware to block a ransom in exchange for a file) and remote code execution. Access Points That Lack MFA Are Level 1 Risk.

2) The Warehouse Staff using Inventory Management System can be a victim of this as Cybersecurity is low key and less awareness in Warehouse Staff using the Inventory Management System. Abuse, or phishing, could insert spurious data, creating logistical havoc.

3) Introduction One of the vulnerability points of the GPS fleet system is data spoofing from outsiders, where attackers can generate false data to use on the fleet system. The absence of encrypted transmissions or real-time alerts could allow attackers to alter fleet positions and routes.

4) Customer Data leaks are not only violations of privacy law (eg Privacy Act 1988), but they are also trust destroyers; Zenith’s now-standard practice of enabling shared access for customer handling teams exposes these records.

5) Weak vendor system integration and lack of end-to-end transaction monitoring expose Financial Logs. That opens up the possibility for invoice tampering or fraudulent transfers.

6) The Supplier Portal doesn't provide strong authentication or encrypted data transport channels. Which enables eavesdropping, or business disruption through false orders or delayed procurement.

7) HR Systems collect confidential personal data. No audit trails, vague user roles, high chances of insider threats or misuse.

Likelihood & Impact Analysis

Using the OCTAVE framework, we carried out a likelihood-impact assessment for the seven most critical information assets in Zenith Logistics. It assesses the likelihood of threats, as well as the business impact of those threats. A 5x5 risk matrix visually presents your risk exposure levels, allowing you to plan mitigation methods based on risk priority.

Asset	Likelihood (L)	Impact (I)	Risk Score (L × I)	Risk Level
LogiFlow Database	5 (Very Likely)	5 (Severe)	25	**Extreme**
Inventory Management System	4 (Likely)	4 (High)	16	**High**
GPS Fleet Tracking System	3 (Possible)	4 (High)	12	**Moderate–High**
Customer Order & Profile Data	4 (Likely)	5 (Severe)	20	**Extreme**
Financial Transaction Logs	3 (Possible)	5 (Severe)	15	**High**
Supplier Coordination Portal	3 (Possible)	3 (Moderate)	9	**Moderate**
Employee Records & HR System	2 (Unlikely)	4 (High)	8	**Moderate**

Risk Score Legend:
1–5: Low | 6–10: Moderate | 11–15: High | 16–25: Extreme

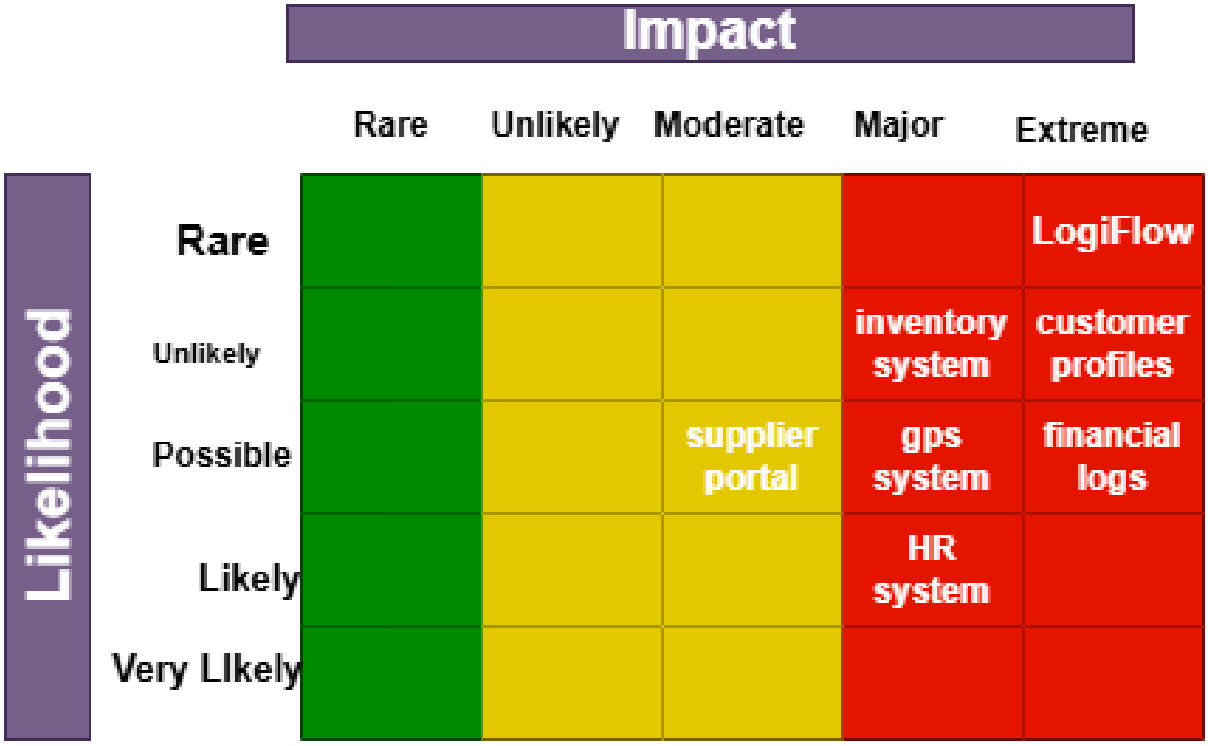

Figure 2: Risk matrix (**created using draw.io**)

Risk Evaluation, Prioritisation & Mitigation Strategy

Priority	Asset	Risk Description	Risk Score	Mitigation Strategy	Recommended Controls (P/D/C)
1	LogiFlow Database	Ransomware, data loss, unauthorized access	25	Implement Zero Trust Architecture (ZTA)	Preventive: MFA, network segmentation Detective: Activity logging Corrective: Daily off-site backups
2	Customer Order & Profile Data	Privacy breaches, identity theft	20	Data Classification & Access Control Policy	Preventive: Role-based access, data encryption Detective: Audit logs Corrective: User activity review
3	Inventory Management System	Tampered inventory records, phishing	16	Phishing Simulation & Staff Training Program	Preventive: Security awareness training Detective: Suspicious login alerts Corrective: Policy re-education
4	Financial Transaction Logs	Invoice fraud, financial manipulation	15	Transaction Integrity Monitoring (TIM)	Preventive: Segregation of duties Detective: Reconciliation audits Corrective: Incident response SOPs
5	GPS Fleet Tracking System	Data spoofing, route manipulation	12	Endpoint Security Management (ESM)	Preventive: Encrypted GPS traffic Detective: Location anomaly detection Corrective:

					Emergency reroute procedures
6	Supplier Coordination Portal	Unauthorized orders, data leaks	9	Secure API Gateway & Partner Verification	Preventive: API key management Detective: Monitoring unusual supplier actions Corrective: Auto-disconnect suspicious sessions
7	Employee Records (HR System)	Internal misuse, payroll data leaks	8	Privileged Access Management (PAM)	Preventive: Least-privilege enforcement Detective: Access audits Corrective: Role-based access adjustment

Justification of priority order

1) All logistics functions are central to LogiFlow Database. A compromise would shut down operations completely, affecting multiple departments at once.
2) Once again, Customer Data is one of the product data that is governed by privacy laws, being a major reputational and legal liability if exposed.
3) Logistics accuracy, client deliveries and order management are all directly affected by Inventory Data. Low-security endpoints with phishing threats increase the likelihood score.
4) Widespread third-party integration causes fraud and accounting mistake in financial logs.
5) A disruption in delivery schedules could also result in customer service challenges.
6) Supplier Portal also runs a moderate risk because it isn't a system used as frequently as others, but it still threatens business continuity when misconfigured or misused.
7) HR System has sensitive data, however, incidents are largely internal and less disruptive to operations

Conclusion

This cybersecurity assessment has revealed that Zenith Logistics operates with significant vulnerabilities across its core systems, particularly in the LogiFlow database, customer data handling, and financial processes. Through the application of the OCTAVE framework, the organization's top risks have been identified, evaluated, and prioritized based on likelihood and impact.

To strengthen its cybersecurity posture, Zenith must take immediate action on the recommended mitigation strategies, beginning with Zero Trust architecture, multi-factor authentication, and organization-wide staff training. These measures will not only address current vulnerabilities but will also build resilience against future cyber threats.

Securing these critical assets is essential to preserving operational continuity, protecting sensitive data, and maintaining customer trust. With leadership support and a proactive risk management approach, Zenith Logistics is well-positioned to achieve a secure and scalable digital future.

References

1. Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: The OCTAVE approach*. Addison-Wesley.
2. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. https://www.nist.gov/cyberframework
3. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. ISO.
4. Australian Cyber Security Centre. (2023). *Strategies to mitigate cybersecurity incidents: The Essential Eight*. https://www.cyber.gov.au
5. Office of the Australian Information Commissioner. (2023). *Guide to securing personal information*. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information
6. Microsoft. (2022). *Zero Trust security model*. https://www.microsoft.com/en-us/security/business/zero-trust
7. Diagrams.net. (2024). *Draw.io – Free online diagram editor*. https://www.draw.io
8. Google Workspace. (2023). *Google Style Guide for Docs & Presentations*. https://workspace.google.com/
9. Australian Government. (1988). *Privacy Act 1988*. https://www.legislation.gov.au/Details/C2023C00137
10. Swinburne University of Technology Library. (2024). *APA referencing style guide (7th edition)*. https://www.swinburne.edu.au/library/referencing/apa-style-guide/

Appendix

“Appendix A: Information Asset Inventory”

Category	Asset Name	Description	Type	Value / Sensitivity	Used In
Customer Data	Customer Profiles	Full customer details (names, contact, billing, delivery instructions)	Logical	High	Customer Order Processing, CRM
Customer Data	Order History	Previous purchases, frequency, volume	Logical	Medium	CRM, Business Intelligence
Supplier Information	Supplier Contracts	Agreements, SLAs, terms	Logical	High	Supplier Coordination System
Supplier Information	Product Specs & Payment Logs	Technical & financial supplier records	Logical	High	Procurement, Inventory
Logistics Operations	LogiFlow Database	Central SCM system (shipment, inventory, routes, orders)	Logical	Very High	Core Logistics System
Logistics Operations	GPS Fleet Tracking Data	Real-time location data, route logs	Logical	Medium	Transportation & Delivery Management
Logistics Operations	Inventory Data	SKU data, stock levels, expiry dates	Logical	High	Warehouse System, Auto Reorder
Logistics Operations	Shipping Logs	Carrier details, timestamps, delivery confirmations	Logical	High	Reporting, Customer Service

IT & Infrastructure	On-Premises Servers	Hosts LogiFlow and finance systems	Physical	Very High	Core IT Infrastructure
IT & Infrastructure	Cloud HR & Payroll Systems	Employee data, pay details (SaaS)	Logical	High	HR Management
IT & Infrastructure	Network Devices	Routers, switches, VPN appliances	Physical	Medium	Secure Access Management
Security Data	System Access Logs	Login records, failed attempts, VPN logs	Logical	High	Incident Response, Auditing
Security Data	Firewalls & Endpoints	Security configurations, alerts	Logical	Medium	Network Security Monitoring
Financial Records	Invoices & Transactions	Customer and supplier payments	Logical	High	Finance System
Financial Records	Customs & Tax Documentation	International shipping, tax compliance	Logical	Medium	Legal, Accounting
Employee Data	Payroll Records	Salaries, hours, deductions	Logical	High	HR System
Employee Data	Training History	Security awareness, compliance modules	Logical	Medium	HR System, Compliance
Employee Data	Work Schedules	Shift allocations	Logical	Low	Operations
Communication & Docs	Internal Email Server	Staff communication history	Logical	High	All business units
Communication & Docs	Shared Drives & USBs	File storage, document transfers	Physical & Logical	Medium	General use, Warehousing