Executive Summary:

This report presents the findings and recommendations of a cybersecurity risk assessment conducted for Jungle Kitchen, a small-scale food manufacturing enterprise undergoing digital transformation. The objective of this assessment was to identify critical assets, evaluate associated cybersecurity risks, and propose cost-effective mitigation strategies, aligning with the organization's operational goals.

The assessment was carried out using the **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)** framework, which emphasizes organizational awareness, asset-based risk identification, and strategic risk mitigation. Jungle Kitchen's key digital assets include:

- Business laptops used for daily operations
- Google Drive, which stores sensitive business and staff-related information
- Gmail accounts used for internal and external communication
- A Wix-based website integrated with a payment portal
- Staff-owned BYOD (Bring Your Own Device) endpoints
- Cloud-based backups hosted on Google Cloud

Through the assessment, several risks and vulnerabilities were identified. Notably, the organization lacks multi-factor authentication (MFA) across critical services, does not enforce encryption for data in storage or transit, and has not implemented formal cybersecurity policies or training programs. Moreover, the absence of regular backup testing and over-reliance on a single backup location present a threat to business continuity in the event of data loss or system failure.

Despite existing controls such as WPA2-secured Wi-Fi, regularly updated antivirus software, and role-based access restrictions on cloud storage, significant gaps remain in governance, access control, and threat detection.

The following key recommendations are proposed:

1. **Implement Multi-Factor Authentication (MFA)** across all accounts and cloud services to strengthen access control.
2. **Develop and enforce formal cybersecurity policies** covering password hygiene, device usage, data classification, and incident response.
3. **Conduct cybersecurity awareness training** for all staff, with an emphasis on phishing prevention and secure file handling.
4. **Enhance data backup practices** by establishing geographically diverse storage locations and regularly testing data recovery processes.
5. **Perform third-party security reviews** of the Wix-based website and define clear roles and responsibilities regarding its maintenance.
6. **Introduce encryption mechanisms** for both data at rest and in transit to ensure confidentiality and compliance with best practices.

By adopting the above measures, Jungle Kitchen will significantly reduce its cybersecurity risk exposure while improving operational resilience and customer trust. The proposed approach is designed to be scalable, practical, and appropriate for the organization's current size and technical capacity.

Technical Analysis

1. Organizational Background

Jungle Kitchen is a micro/small-scale food manufacturing enterprise with two primary locations (Singapore and Sri Lanka). The organization is currently in its early digital transformation stage and relies on cloud-based tools such as Google Drive, Gmail, and a Wix-based e-commerce website for business operations. The organization comprises 25 employees and utilizes both company-owned and personally-owned (BYOD) devices to manage workflows. While the organization demonstrates commitment to adopting secure tools, it currently operates with minimal cybersecurity governance.

2. Identification of Critical Assets (OCTAVE Phase 1)
In accordance with the OCTAVE methodology, Jungle Kitchen's critical information assets were identified based on their importance to daily operations and their sensitivity to potential security incidents. These assets form the foundation upon which further risk analysis and mitigation strategies are built. The following table summarizes each asset, its role within the organization, and the justification for its classification as critical:

Asset Name	Description	Why It's Critical
Google Cloud Drive	Used to store staff documents, operational files, and other sensitive data	Contains essential business and personal information that supports day-to-day operations
Laptops	Recognized as the organization's most vital digital tools	Primary devices used for accessing cloud services, communication, and managing business workflows
Wix-Based Website with Payment Portal	Main web application maintained by a third party	Facilitates customer payments and acts as a central platform for the company's online presence
Email Accounts	Used for internal and external communication across teams	Essential for operational coordination, file sharing, and cloud service authentication
BYOD Staff Devices	Staff-owned personal devices used for work-related tasks	These devices interact with company data but are not centrally managed, increasing security exposure
Cloud-Based Backups	Weekly backups stored on Google Cloud	Serve as the organization's primary disaster recovery mechanism in the event of data loss or breach

This asset inventory is a prerequisite for determining risk exposure, developing threat profiles, and allocating protective controls. Each of the listed assets was later assessed for its confidentiality, integrity, and availability requirements as per OCTAVE's next phase

3. Security Requirements (OCTAVE Phase 2)

Each identified asset was evaluated against the three fundamental security principles: **Confidentiality (C), Integrity (I), and Availability (A).** The goal is to understand how essential each principle is to the asset's proper functioning and to support risk-based decision-making in later phases.

Asset	Confidentiality	Integrity	Availability	Justification
Google Cloud Drive	High	High	Medium	Stores operational and potentially sensitive personal and business data. Unauthorized access or tampering may lead to privacy violations or data loss.
Company Laptops	High	Medium	High	Used to access and manage all digital operations. Loss or compromise can result in both operational downtime and data leakage.
Wix Website & Payment Portal	High	High	High	Handles customer payments and public presence. Requires all three pillars to protect user trust and ensure business continuity.
Email Accounts (Gmail)	High	High	Medium	Core communication tool. Compromise could expose confidential information or allow attackers to pivot to other systems.
BYOD Staff Devices	Medium	Medium	Medium	Used for accessing organizational services. Potential data leaks or loss from personal device misuse or compromise.
Cloud-Based Backups	High	Medium	High	Vital for recovery from disasters or cyber incidents. Loss or corruption of backups would severely impact business continuity.

This CIA analysis guides the prioritization of security controls such as encryption, MFA, backup redundancy, and access restriction.

4. **Threat Identification & Vulnerability Analysis**

Each asset was analyzed in terms of common threats, system weaknesses, and the impact such events would have on Jungle Kitchen's operations. The following table summarizes the threat landscape:

Threat Profile Table

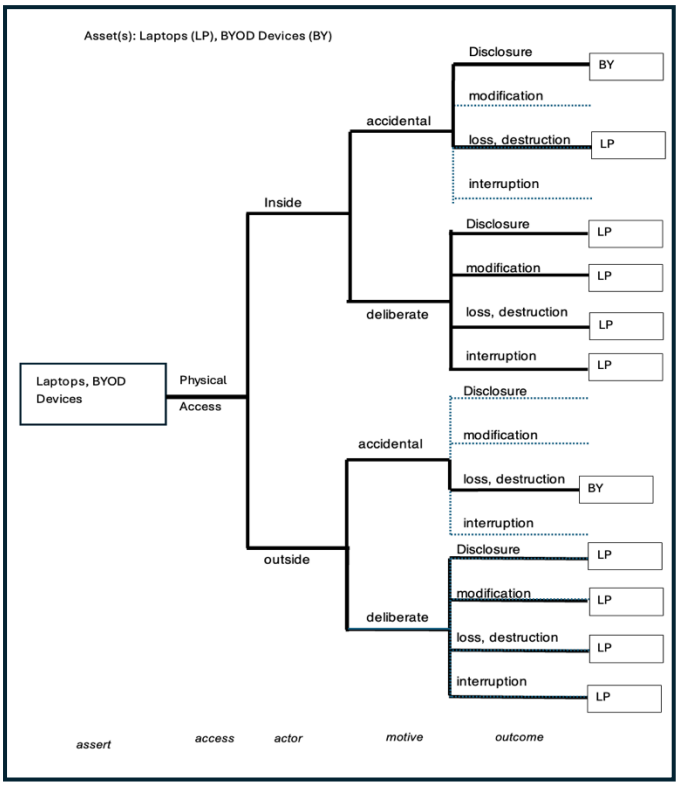
Asset	Threat	Vulnerability	Impact on Organization
Google Cloud Drive	Unauthorized access or data breach	No encryption (Q5.2), limited access controls	Exposure of sensitive staff; privacy/legal issues
Laptops	Malware infection or theft	Default password settings (Q4.2), lack of endpoint	Operational disruption; potential unauthorized access to cloud and email

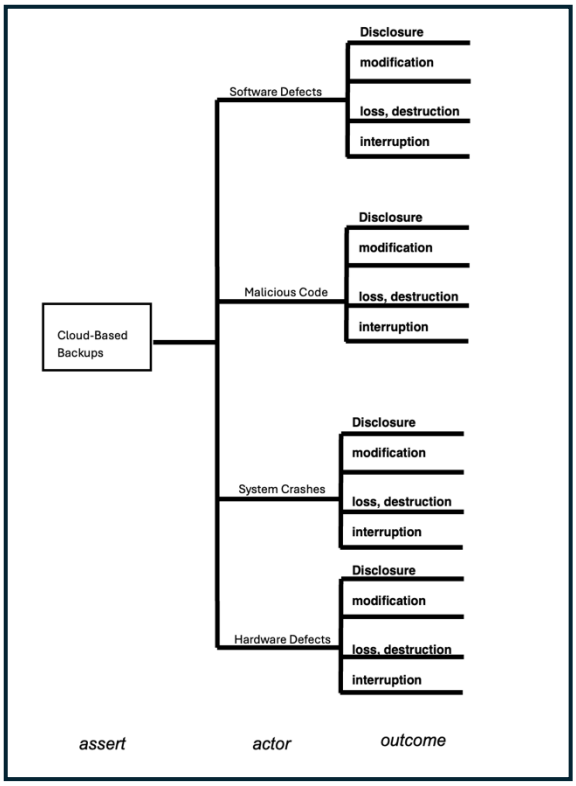
		hardening, no asset tracking	
Wix Website with Payment Portal	Website compromise, defacement, or payment skimming	Third-party managed (Q12.2), no internal control or code review	Financial loss; reputational damage; trust issues with customers
Email Accounts	Phishing attacks or credential theft	No enforced MFA (Q4.2), no awareness training (Q8.1), no monitoring (Q17.1)	Unauthorized access to sensitive communication; potential compromise of cloud accounts
BYOD Devices	Data leakage, device loss or misuse	No plan for lost devices (Q14.3), weak control over personal device access	Breach of organizational data; potential regulatory violations
Cloud-Based Backups	Data loss or failed recovery	No backup testing (Q6.2), single backup location (Q6.3)	Inability to restore operations after an incident or attack

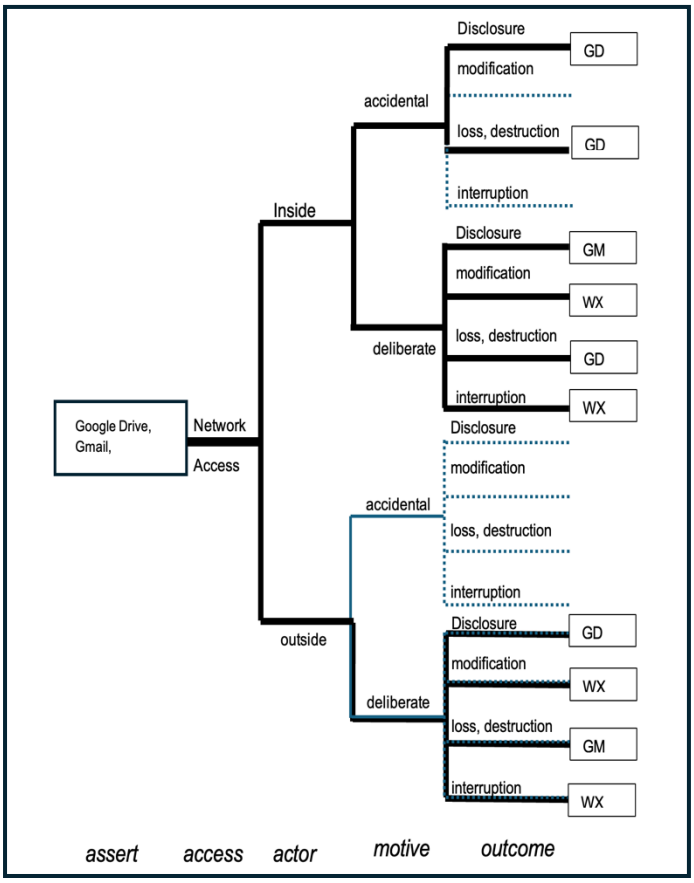
Organizational Vulnerabilities Table

Area	Observed Vulnerability	Evidence from Data
Cybersecurity Policies	No formal written policies (e.g., acceptable use, data classification, password policies)	Q2.1 – "No"
Policy Acknowledgment	Staff are not required to read or acknowledge security policies	Q2.2 – "No"
Information Security Governance	No Data Protection Officer or Security Officer assigned	Q2.3 – "No"
Data Encryption	Data is **not encrypted** during storage or transmission	Q5.2 – "No"
Backup Practices	Backups are not tested for recovery; only stored in cloud	Q6.2 – "No"; Q6.3 – "Google Cloud only"
Incident Response	No history of incident handling; incident response plan exists but not practiced	Q7.1 – "No incidents"; Q7.3 – "Yes", but no evidence of implementation
Access Control	Accounts are managed manually; no enforced password policies	Q4.1 – "Manually"; Q4.2 – "Windows default"
BYOD Security	No clear plan in place if staff device with data is lost; only antivirus is enforced	Q14.2 – "Antivirus only"; Q14.3 – "No plan
Training and Awareness	No current cybersecurity training for staff	Q8.1 – "Yes (future plan)"; not implemented yet
Monitoring and Logging	No system or network activity monitoring tools in place	Q17.1 – "A bit"; Q17.2 – "No experience with SIEM tools"
MFA Adoption	MFA is not confirmed across all systems	Q4.2, Q14.3 – no clear enforcement
Physical Security	No CCTV or visitor logbook system currently used	Q9.2 – "No, but planning"
Third-Party Risk Management	No evaluations of third-party vendors for security practices	Q13.3 – "No"
Legal & Compliance Awareness	Not aware of Sri Lanka's Personal Data Protection Act	Q16.1 – "No"
Secure Data Disposal	No secure disposal practices for physical or digital records	MSME intake Q4 – "No"

Threat Tree Diagrams







Proposed Security Architecture

The following architecture is proposed to enhance Jungle Kitchen's cybersecurity posture while remaining practical and cost-effective for a small business. The design is based on the critical assets and vulnerabilities identified through the OCTAVE assessment.

Key Components:

- Wi-Fi Network: WPA2 secured, limited to known devices only.
- Laptops: Protected by antivirus (Kaspersky), encrypted hard drives, and strong password enforcement.
- BYOD Devices: MDM-enforced, limited to work-related access with remote wipe capability.
- Google Services:
  - Drive and Gmail protected with MFA, role-based access control, and link sharing restrictions.
    - Wix Website: Third-party maintained, with admin credentials secured via MFA and password manager.
    - Backups: Weekly Google Cloud backups plus local encrypted offline backup (e.g., portable hard drive).

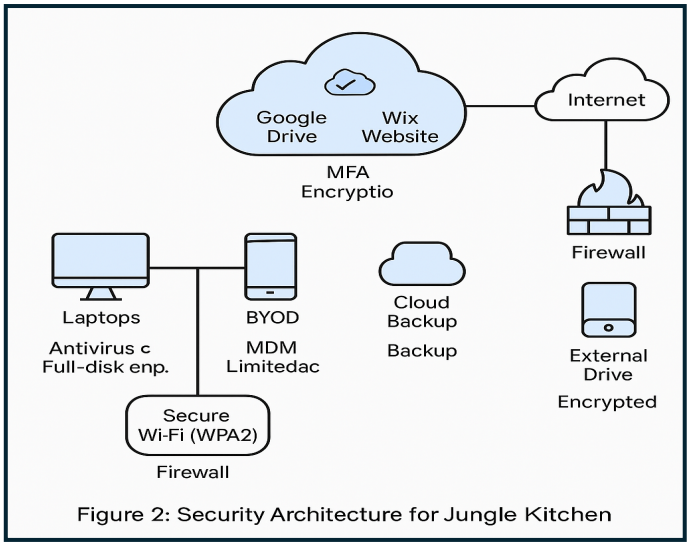


Figure 2: Security Architecture for Jungle Kitchen

Security Controls Summary:

Component	Control Applied
Laptops	Antivirus software, full-disk encryption, strong password policies
BYOD Devices	Mobile Device Management (MDM), restricted access policies, antivirus
Wi-Fi Network	WPA2 encryption, hidden SSID, MAC address filtering
Google Drive/Gmail	Multi-Factor Authentication (MFA), link-sharing control, access logging
Wix Website	Admin credentials secured with MFA, regular third-party audits

Backups	Weekly cloud backups, encrypted external drive, recovery testing

Technical Staff Summary:

This section provides a prioritized action plan for Jungle Kitchen's technical personnel to implement the recommended cybersecurity enhancements. The goal is to address critical risks while remaining practical, cost-effective, and scalable for a small business context.

Implementation Priorities:

1.Enable Multi-Factor Authentication (MFA):
- Apply MFA to Gmail, Google Drive, and Wix admin accounts.
- Use authenticator apps or hardware tokens.

2.Initiate Staff Cybersecurity Training
- Cover phishing, password hygiene, and secure data handling.
- Repeat every 3–6 months.

3.Upgrade Laptop and BYOD Security:
- Enforce disk encryption, antivirus, and OS updates on laptops.
- Apply MDM policies to control personal device access.

4.Review Cloud Access and Permissions:
- Audit Google Drive link sharing and enforce role-based permissions.

5. Secure the Website and Payment Portal
- Request a third-party audit of the Wix setup.
- Ensure admin access is limited and protected.

6.Enhance Backup Strategy:
- Add a secondary backup location (e.g., encrypted external drive).
- Test backup restoration procedures regularly.

Suggested Tools/Resources:
- Google Workspace Admin tools (for MFA and Drive control)
- Kaspersky or Bitdefender (antivirus)
- Google Endpoint Management or Microsoft Intune (MDM)
- Free phishing training: Google Security Awareness Training or KnowBe4 Free Tier

Recommended Timeline:

Week	Task
1–2	Enable MFA, initiate training
3–4	Upgrade laptop security, BYOD controls
5	Audit Google Drive & Wix admin settings
6	Add backup drive, perform recovery test

References:

[1] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley Professional, 2002.

[2] National Institute of Standards and Technology (NIST), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Rev. 2, Dec. 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[3] Google Workspace Admin Help, “Set up 2-Step Verification (MFA),” [Online]. Available: https://support.google.com/a/answer/175197?hl=en

[4] Wix Help Center, “Site Security Guidelines,” [Online]. Available: https://support.wix.com/en/article/security-at-wix

[5] KnowBe4, “Free Cybersecurity Awareness Training,” [Online]. Available: https://www.knowbe4.com/free-training-resources

[6] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*, International Organization for Standardization, 2013.

Appendix A – Threat Tree Diagrams

Figure A1: Threat Tree – Google Drive

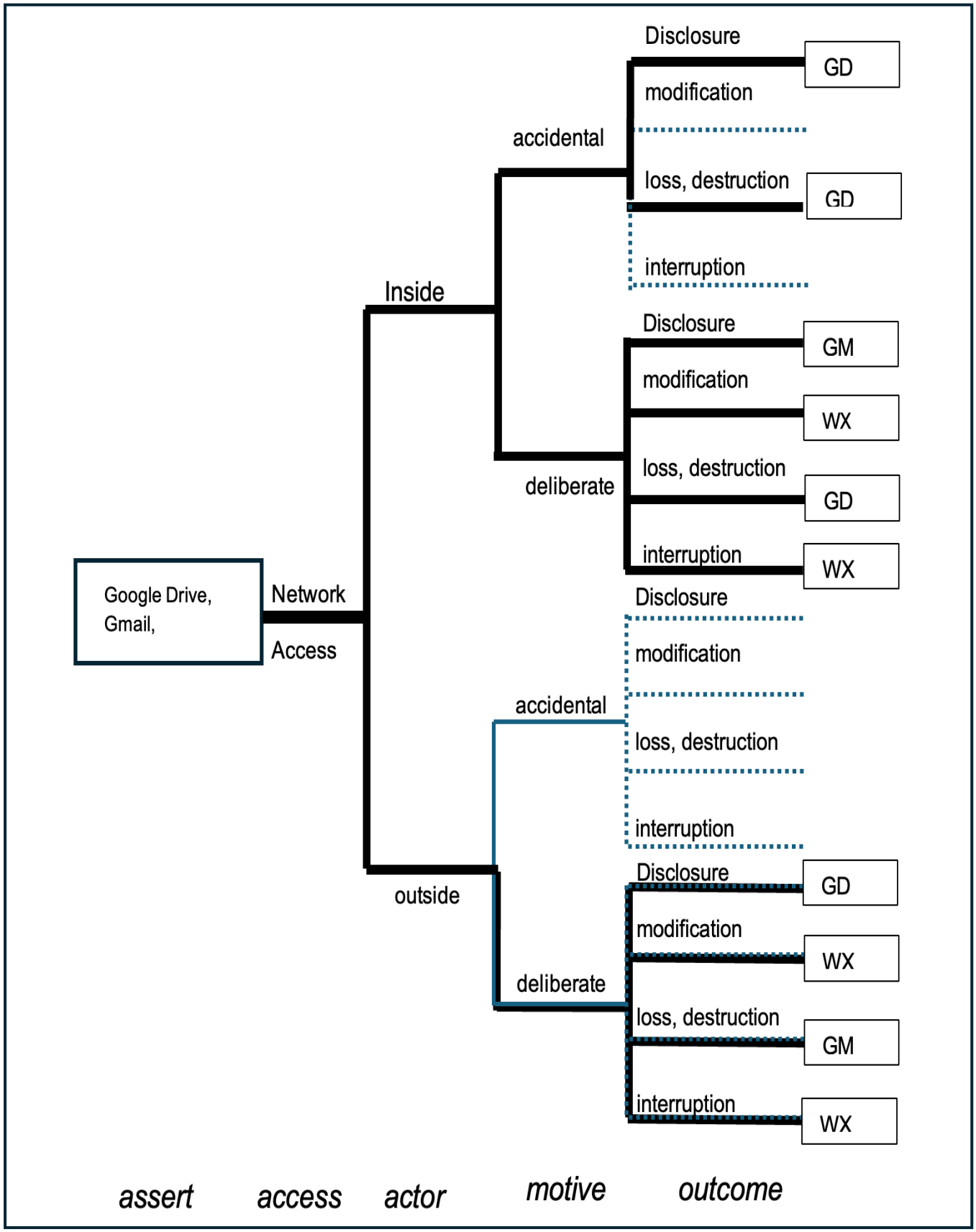


Figure A2: Threat Tree – Laptops & Email

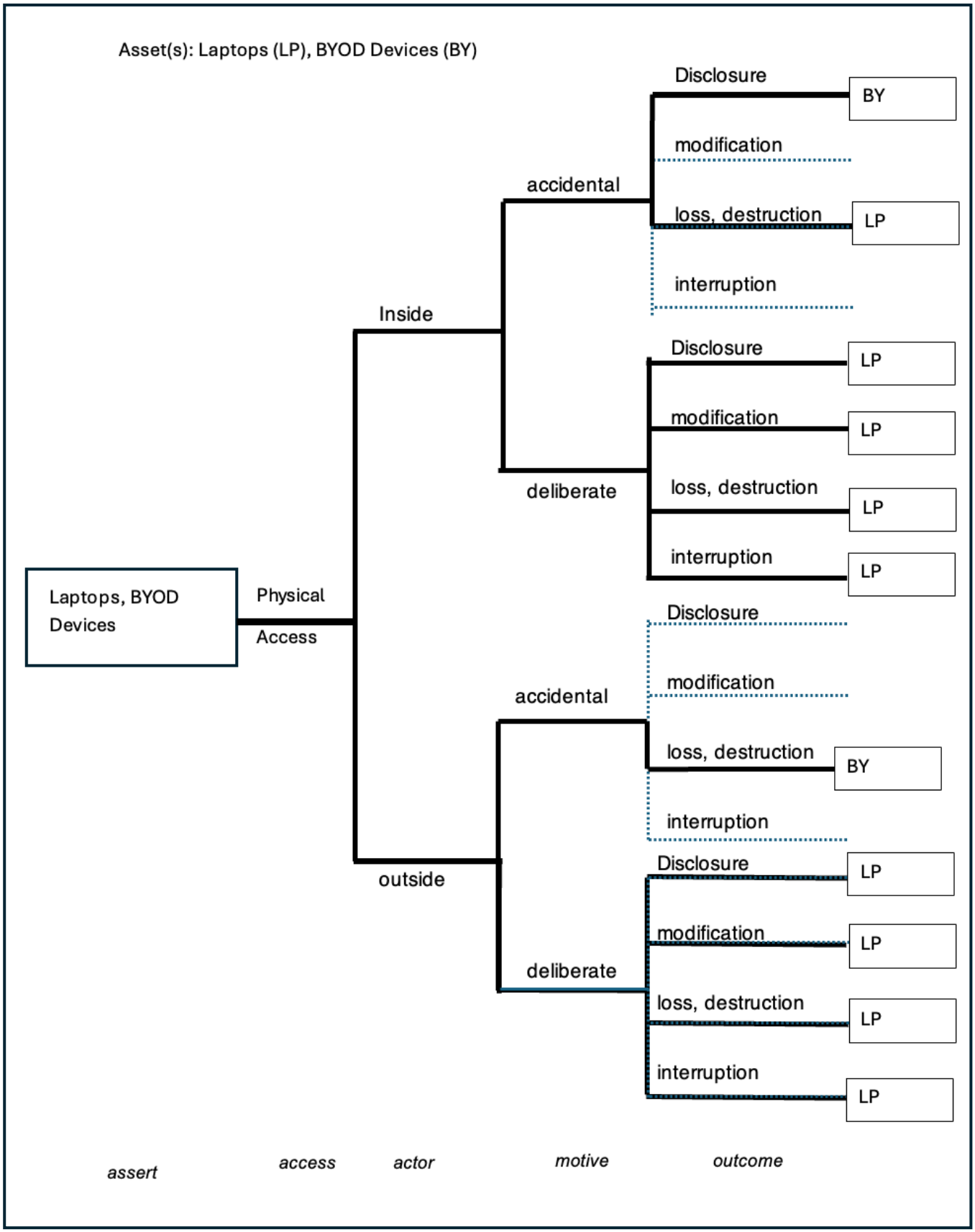
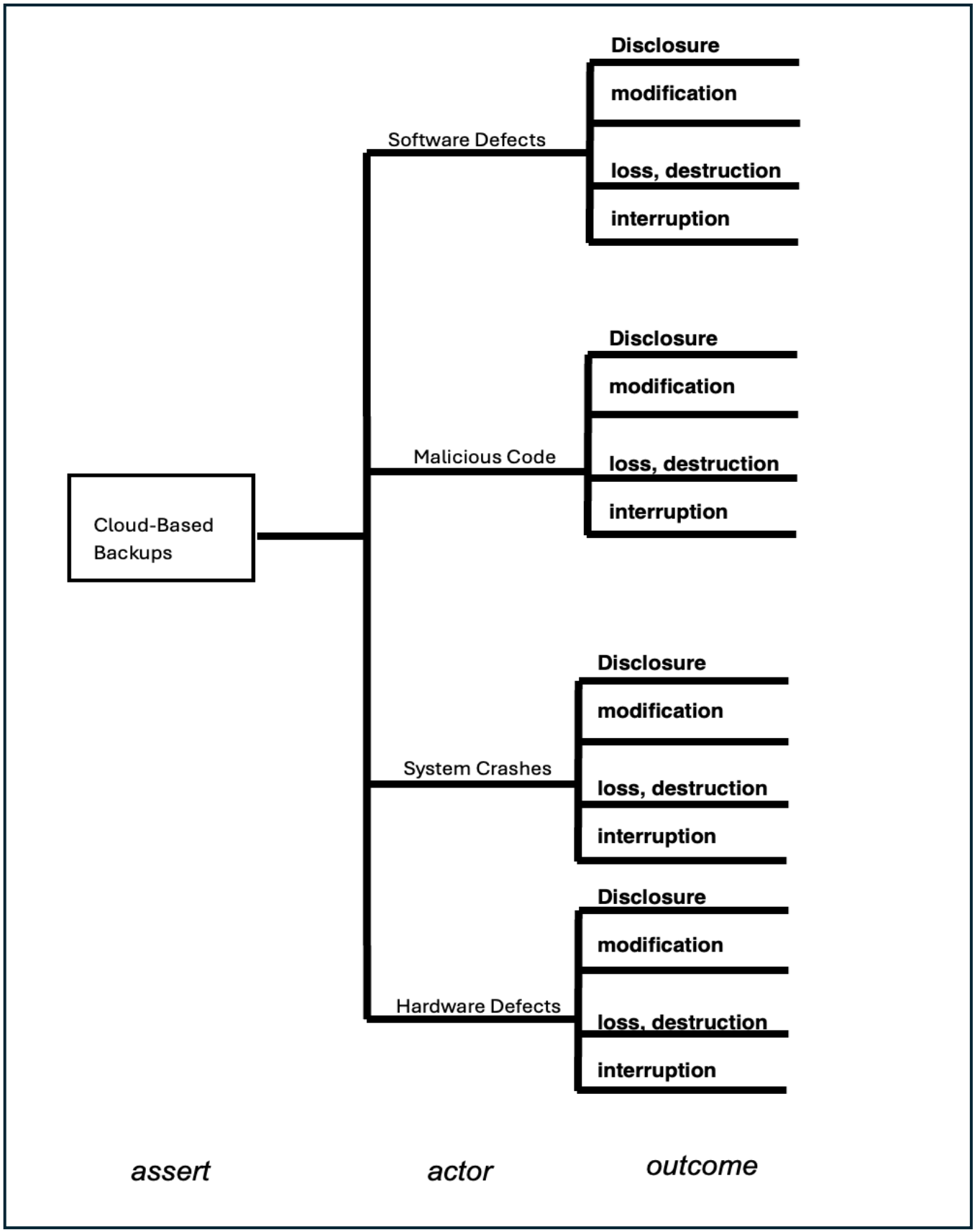


Figure A3: Threat Tree – BYOD & Backups



Appendix B – Security Architecture Diagram

Figure B1: Proposed Security Architecture for Jungle Kitchen