PEPSICO

Ameen Rufai, Tyree Black, Saniya Isaac, Antonette Simms, Hamza Amadu

Company Overview

- **Founded**: PepsiCo was founded in 1965 through the merger of Pepsi-Cola and Frito-Lay.
- **Headquarters**: Purchase, New York, United States.
- **Industry**: Food and Beverage.
- **Products**: PepsiCo produces a wide range of beverages, including soft drinks (e.g., Pepsi, Mountain Dew) and non-carbonated beverages (e.g., Gatorade, Tropicana), as well as snacks and food items (e.g., Lay's chips, Quaker Oats).
- **Global Reach**: PepsiCo operates in over 200 countries and territories worldwide.
- **Revenue**: As of the last update, PepsiCo's annual revenue is in the tens of billions of dollars, making it one of the largest food and beverage companies globally.
- **Employees**: PepsiCo employs tens of thousands of people worldwide, across various functions including manufacturing, distribution, marketing, and research and development.
- **Commitment to Sustainability**: PepsiCo has made commitments to sustainability, including goals to reduce its environmental impact, improve water efficiency, and promote healthier product options.

Network topology

Physical Topology:

PepsiCo's network is physically structured with wired and wireless connections.

Main components:

- Ethernet cables connecting devices within sites.
- Fiber optic cables linking data centers and remote sites.
- Wireless access points providing Wi-Fi connectivity.

Star Topology

- Routers managing inter-site traffic.
- Switches aggregating and controlling traffic flow at regional offices.
- End Devices: Switches connecting end-user devices at each site.

Network Devices & Security Measures:

Network devices include switches, routers, firewalls, and intrusion detection/prevention systems.

Security measures implemented align with NIST guidelines, encompassing encryption, access control, intrusion detection/prevention, and network segmentation.

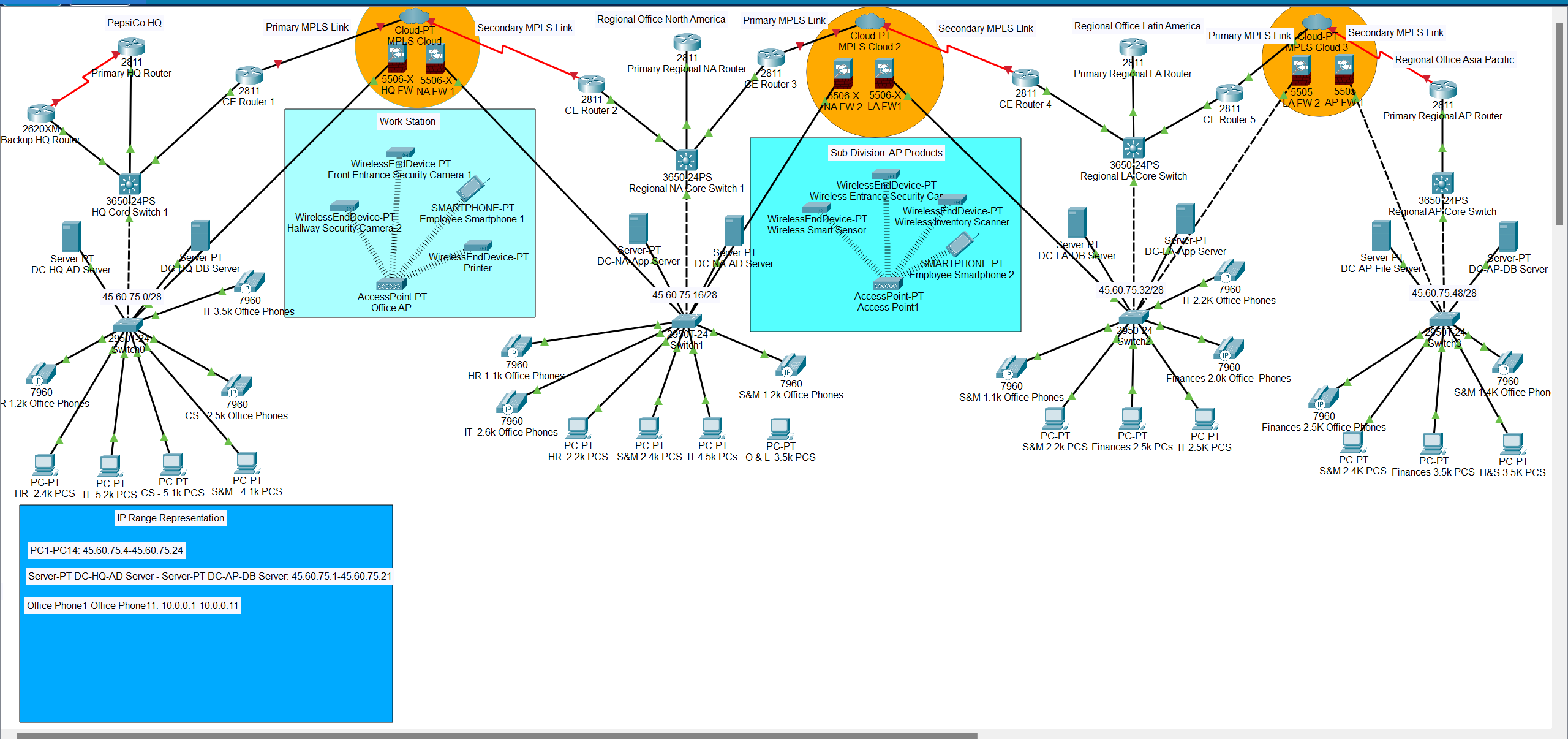
Additional Components:

Power Over Ethernet (PoE) switches powering wireless access points and IP phones.

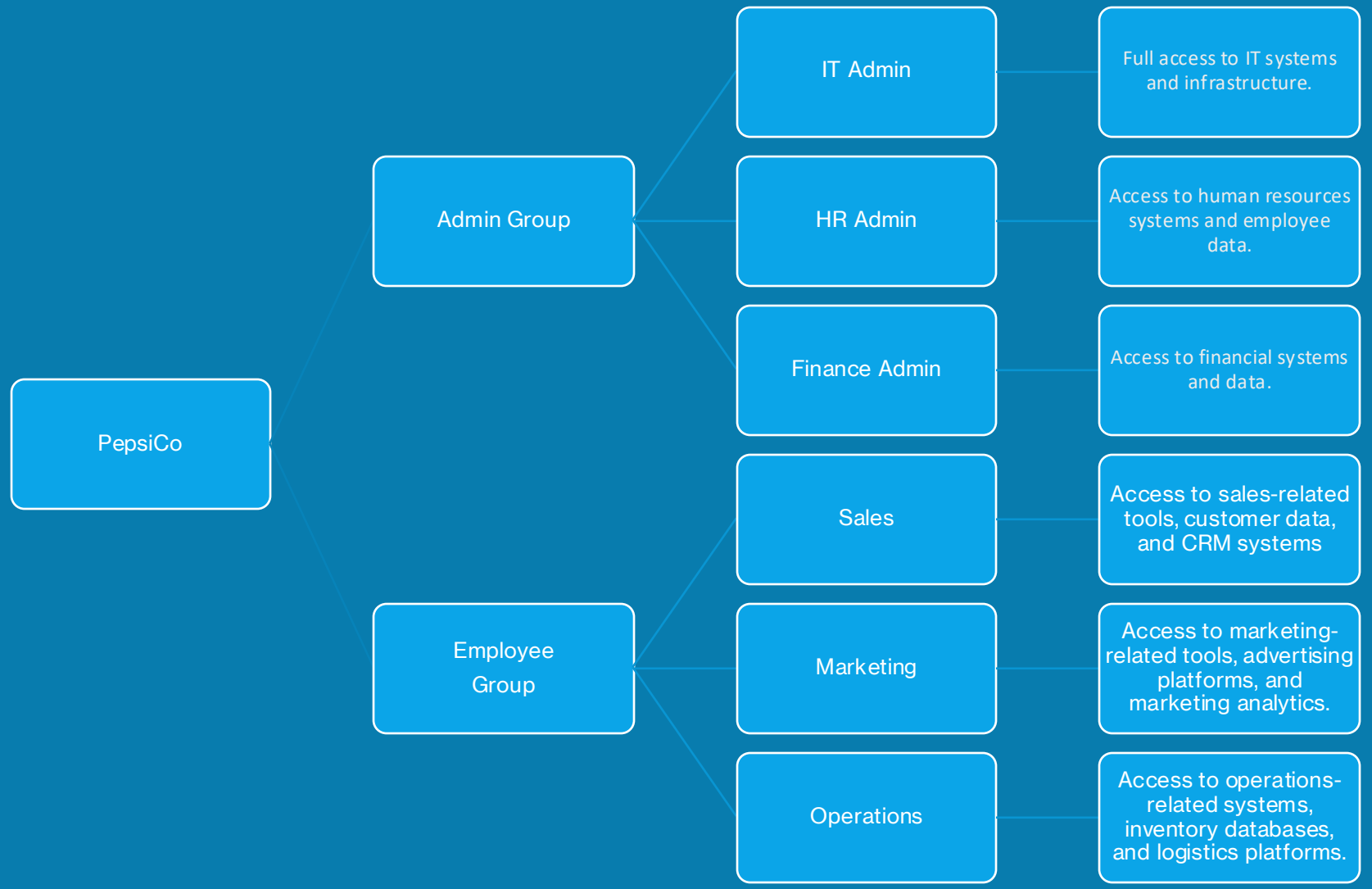
UPS (Uninterruptible Power Supply) units providing backup power.

Cable management systems ensuring neat and organized wiring infrastructure.

Network Diagram



Access Control Management & Controls



Vulnerability Assessment

Employees:

- **Vulnerabilities**: Phishing attacks, social engineering, insider threats, weak password practices.
- **Mitigation**:
  - Regular cybersecurity awareness training.
  - Implementation of multi-factor authentication (MFA).
  - Strong password policies and access controls.

Products (Beverages & Snacks):

- **Vulnerabilities**: Product tampering, counterfeiting, supply chain attacks.
- **Mitigation**:
  - Rigorous supply chain management practices.
  - Tamper-evident packaging and tracking mechanisms.
  - Audits and inspections along the supply chain.

Supply Chain Information:

- **Vulnerabilities**: Third-party breaches, data leaks, supply chain disruptions.
- **Mitigation**:
  - Thorough risk assessments of supply chain partners.
  - Encryption and access controls for sensitive data.
  - Incident response plans for disruptions and breaches.

Customer Data:

- **Vulnerabilities**: Data breaches, unauthorized access, data loss.
- **Mitigation**:
  - Encryption of customer data and access controls.
  - Monitoring and auditing of access to customer databases.
  - Compliance with data protection regulations.

Recipes & Marketing Strategies:

- **Vulnerabilities**: Intellectual property theft, unauthorized access.
- **Mitigation**:
  - Secure storage and encryption of sensitive information.
  - Access controls and authentication mechanisms.
  - Monitoring and logging of access to protect against unauthorized access.

Vulnerabilities and Protection of Marketing Strategies

- **vulnerabilities:**
- Social Engineering Attacks:
  - Phishing emails targeting social media managers.
  - Spear phishing exploiting knowledge of marketing strategies.
- Unauthorized Access:
  - Weak or reused passwords for social media accounts.
  - Lack of two-factor authentication.
- Data Breaches:
  - Insecure storage leading to potential leaks.
  - Unauthorized access to customer data.
- Malware Infections:
  - Clicking on malicious links or attachments.
  - Malvertising campaigns targeting social media users.
- **Protection Measures:**
- Employee Training:
  - Regular cybersecurity awareness sessions.
- Strong Authentication:
  - Implement two-factor authentication (2FA).
- Access Control:
  - Role-based access control (RBAC) for document access.
- Encryption:
  - Encrypt sensitive marketing data at rest and in transit.
- Endpoint Security:
  - Deploy endpoint protection solutions.
- Incident Response Plan:
  - Develop and test a specific incident response plan.
- By implementing these measures, PepsiCo can secure its marketing strategies and mitigate potential risks effectively.

Introduction to NIST framework

- Purpose of NIST Framework:
  - Structured approach to managing cybersecurity risk.
  - Helps identify, protect, detect, respond to, and recover from cyber threats.
- Importance in PepsiCo's Network Security:
  - Ensures alignment with industry best practices and regulatory compliance standards.
  - Facilitates implementation of effective security measures to safeguard PepsiCo's network infrastructure.

NIST framework Overview

- Identify Function:
  - Subcategories: ID.AM-1, ID.AM-5
  - Taking our assets into consideration.
  - Implementation: Utilize network scanning tools to identify and catalog network assets.
- Protect Function:
  - Subcategories: PR-AC-1, PR-AC-2, PR-AC-3, PR.AC-4, PR.AC-5
  - Implementation: Configure access control lists (ACLs) on routers and firewalls to protect network resources.
- Respond Function:
  - Subcategories: RS.RP-1
  - Implementation: Develop incident response plans and conduct tabletop exercises to simulate cybersecurity incidents.
- Recover Function:
  - Subcategories: RC.IM-1, RC.IM-2
  - Implementation: Regularly backup critical network data and establish procedures for restoring services after an incident

NIST framework Overview Cont.

- DE.CM Function:
  - Objectives: Describe cyber defense tools, methods, and components.
  - Implementation: Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and mitigate network attacks.
- DE.AE Function:
  - Goals: Properly respond to system compromises and security incidents.
  - Implementation: Conduct forensic analysis using packet capture tools to investigate security breaches.
- CSP Function:
  - Purpose: Define the principles of cybersecurity.
  - Implementation: Enforce the principle of least privilege by configuring user access levels on network devices.
- BCO Function:
  - Significance: Understand the interaction between security, system usability, and business objectives.
  - Implementation: Conduct security awareness training for PepsiCo employees to educate them on cybersecurity best practices.

Conclusion

- Recap of NIST Framework Functions and Implementations:
  - Identify, Protect, Detect, Respond, Recover.
- Importance for PepsiCo's Network Security:
  - Ensures comprehensive risk management and resilience against cyber threats.
- Takeaways:
  - NIST Framework provides a systematic approach to cybersecurity, essential for maintaining the integrity and availability of PepsiCo's network infrastructure.

References

- About PepsiCo. (n.d.). PepsicoUpgrade. https://www.pepsico.com/who-we-are/about-pepsico
- Cybersecurity and Infrastructure Security Agency (CISA). "Phishing: Overview."
- National Institute of Standards and Technology (NIST). "Multi-Factor Authentication."
- Food and Drug Administration (FDA). "Food Defense."
- United States Computer Emergency Readiness Team (US-CERT). "Supply Chain Risk Management."
- General Data Protection Regulation (GDPR).
- United States Patent and Trademark Office (USPTO). "Intellectual Property Basics."