Organizational Systems and Network Diagram

Ryan Coon

CYB-650

Dr. Howard Goodman

July, 30, 2025

**Introduction**

Technological advancements offer immense opportunities for businesses, enabling enhanced performance through digitalization. Streamlined processes and improved service access lead to faster service times, greater accuracy, and cost optimization. However, this digital transformation also increases the risk of unauthorized access to sensitive data. A cybersecurity risk assessment is crucial for educating employees about potential threats, their impact on various roles, and their likely points of origin. This assessment will analyze Accenture's assets, threats, and vulnerabilities at the organizational level.

Accenture, a global professional services firm, specializes in IT and management consulting. It offers a wide array of services—strategy, consulting, digital, technology, and operations—to enhance organizational performance and value creation. Its assets include both physical (computing devices, hardware) and electronic (data, software) components, varying significantly in value and risk. Comprehensive documentation, including security policies, audit reports, recommendations, and contingency plans (as outlined in the Cybersecurity Framework for Jordan Banking Sector, 2021), is mandatory.

**Technical Requirements**

Minimizing risks requires comprehensive measures. This includes technical training and awareness for all employees to address human-caused risks, effective application controls to handle software failures, and regular monitoring and audits (internal or external). Furthermore, it includes implementing robust data backup and restore processes and adding specialized hardware, such as voice response generation cards, to improve server functionality.

**Hardware Required**

|  |  |
| --- | --- |
| Device Name | Quantity |
| Servers | 11 with 3 main servers |
| Workstations/Laptops | 50 |
| Voice Router | 2 |
| UCS Server | 1 |

**Compliance**

Network segmentation is a key security measure at Accenture, enabling efficient resource allocation and access control, which reduces risks. Each branch, especially those with remote users, employs a Cisco voice router with firewall-based packet filtering. A dedicated Cisco UCS firewall serves as a data center computer in a branch. Local branches also utilize telephony systems, SIP proxy servers, and data/backup servers. All external networking devices are connected to a VoIP gateway, which in turn connects to the VoIP system.

**Related Systems and Assets**

The telephony infrastructure includes customized features, such as a call flow designer, for enhanced functionality. The computing environment primarily comprises Windows-based laptops and HP workstations, integrated with Cisco call center software. High-speed ISDN connections are utilized. SQL Servers operate on SQL Server 2021 with periodic backups. Voice routers are configured with firewall protection and redundancy. Salesforce.com CRM, a cloud-based solution, facilitates comprehensive customer data management, allowing for easy data access and analysis without requiring IT expertise.

**IT Tasks**

IT's responsibilities include keeping all networking devices and systems, including cell phones, current. IT should install enterprise virus protection software on all network-connected devices. VLAN-level IDS/IPS systems are used to filter internet data, monitor for and prevent malicious activity, including reporting and blocking. Mandatory network firewalls are required to prevent security breaches. IT must document and report network issues to maintain PCI compliance. Finally, IT must ensure the availability of BCP, DRP, and regular data backup and restore, in addition to weekly or monthly system performance monitoring.

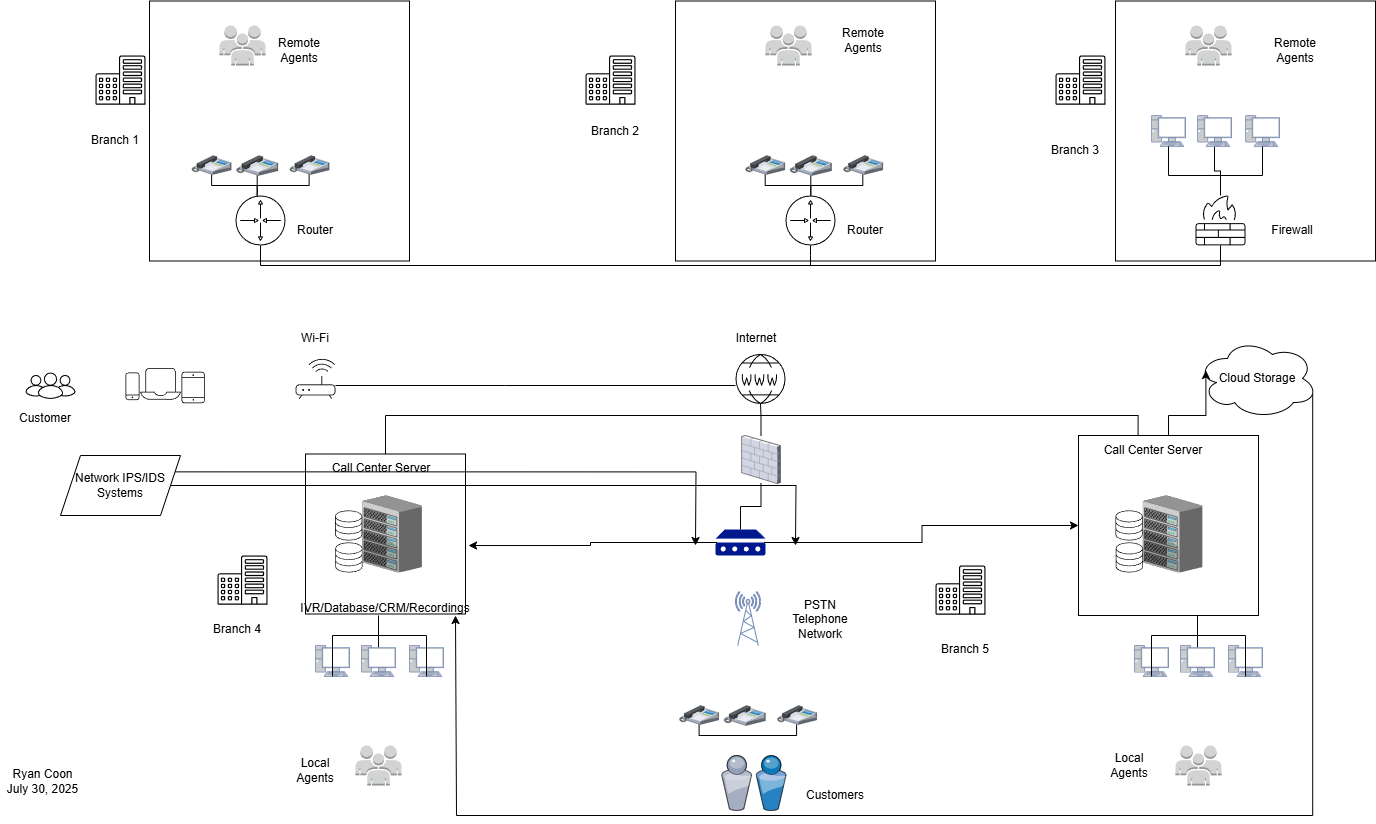
**Implications of the System Connectivity to the Internet**

Data travels securely between routers via a router-to-router VPN. This VPN uses a tunneling protocol (like PPTP or L2TP) to package the data and an encryption protocol (such as MPPE or IPsec) to secure it before transmission across public networks. On Windows, the Connection Manager utility facilitates connections to VPNs and dial-up networks. A firewall provides an additional layer of protection by blocking application-level attacks and malware, ensuring robust network security.

**Data Classification**

For enhanced data security, all hard drives leverage HP Bitdefender encryption. Centralized authentication, authorization, and accounting are managed through RADIUS integration with SQL servers. Network data transmission adheres to a strict Clean Desk Policy, prohibiting handwritten notes and personal documents in the workplace. Access to sensitive customer and payment data is tightly controlled, encompassing both physical access restrictions and integration of recording systems with the CRM. This integration ensures automatic pausing of recordings whenever agents handle sensitive information such as account numbers or security codes. Wireless traffic for local agents is secured through robust encryption, strong passwords, and disabled SSIDs. Multi-factor authentication (MFA) is implemented where necessary, supplementing the automatic three-month password changes for administrative accounts and network devices. This multi-layered approach ensures robust data protection and system security.

**Accenture Network Diagram**

****

This document details the sophisticated network architecture supporting Accenture's inbound call center, a vibrant hub where customer interactions transform into seamless service delivery. The system's foundation rests upon a robust VLAN-based network meticulously designed for Accenture's local agents. Imagine a bustling orchestra: agents, computers, and telecommunication equipment—each a vital instrument—harmoniously collaborate to provide exceptional customer service.

**Voice Traffic Orchestration -**The system elegantly handles both VoIP and PSTN calls. VoIP calls, like digital whispers across the network, are decoded and seamlessly integrated into the PSTN. Conversely, PSTN calls are encoded, transforming into data packets that traverse the IP network with agility. This intricate dance ensures that calls from anywhere are smoothly routed. Tupia's (2010) research underscores the power of the Interactive Voice Response (IVR) system, allowing customers to resolve their queries independently, bypassing frustrating queues.

**Call Routing -** Each call's journey begins with the Public Switched Telephone Network (PSTN), connecting to the Private Automatic Branch Exchange (PABX) via available trunk lines. The caller's identity, revealed through Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS), guides the call's path. Imagine a skilled conductor directing the flow of calls. If all trunk lines are occupied, a busy signal, a brief moment of silence, informs the caller of the momentary congestion. Akhtar and Latif (2010) highlight the crucial role of ANI and DNIS in routing calls to the nearest available agent, based on customer location, creating a remarkably efficient system.

**Security -** Before any internet data reaches the VoIP gateway, it navigates a formidable security system, a multi-layered defense against threats. The integration of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) acts as a vigilant guardian, filtering out malicious traffic, ensuring the system's integrity.

**Customer Data -**Calls are initially routed to the IVR, where customers provide vital information, such as Customer Reference Numbers (CRNs). Agents, equipped with PCs or laptops, access a centralized Corporate Information System, providing them with a comprehensive view of each customer. This integrated approach ensures agents have the information they need to provide personalized and efficient service. The IVR system meticulously collects and matches customer data, allowing agents to seamlessly access both conversation and customer data. This creates a smooth, personalized experience.

**Centralized Management -**At the router-to-router VPN level, the Unified Computing System (UCS) server, fortified by a firewall, serves as a central command center. It integrates computing, networking, and storage resources, streamlining operations and enabling centralized management. Backup and recording servers, both local and cloud-based, guarantee the system's resilience and data integrity. This system is a masterpiece of technological integration, ensuring efficient and secure communication.

References:

Accenture. (2023). *About Accenture*. Accenture.com. https://www.accenture.com/us-en/about/company-index

FINCert. (2021). *Cybersecurity Framework for the Financial Sector - Central Bank of Jordan*. Cbj.gov.jo. https://www.cbj.gov.jo/EN/Pages/Cybersecurity\_Framework\_for\_the\_Financial\_Sector

Salman, Akhtar & Latif, Muhammad. (2010). Exploiting Simulation for Call Centre Optimization. Lecture Notes in Engineering and Computer Science. 2185.  https://www.researchgate.net/publication/45534737\_Exploiting\_Simulation\_for\_Call\_Centre\_Optimization

Tupia, M. (2010). *Information security risks in a customer service call center infrastructure. Guidelines for security managers.* ResearchGate. https://www.researchgate.net/publication/221521613\_Information\_security\_risks\_in\_a\_customer\_service\_call\_center\_infrastructure\_Guidelines\_for\_security\_managers