Design and Implementation of a Secure Company Network System

# Introduction

This document outlines the design and implementation of a secure network system for Cytonn Innovation Ltd, a forward-thinking company specializing in providing innovative cloud solutions globally. The project focuses on creating a robust network infrastructure to support various departments within the organization while ensuring the security of sensitive data and resources.

# Case Study and Requirements

Cytonn Innovation Ltd has a workforce of 600 staff and is preparing to move to a new building with three floors. The building will host various departments, including Sales and Marketing, Human Resources, Finance, ICT, and a Server Room. The ICT department includes Software Developers, Cloud Engineers, Cybersecurity Engineers, Network Engineers, System Administrators, IT Support Specialists, Business Analysts, and Project Managers.

Prior to the move, a new network service needs to be designed and implemented. The company aims to ensure robust security against internal and external threats by implementing a multi-layered security approach, including a firewall with distinct security zones: outside, inside, and DMZ.

# Network Devices Description

# Cisco ASA Firewall

A stack of electronic devices

Description automatically generatedCisco Adaptive Security Appliance (ASA) is a security device that combines firewall, VPN, and other network security services in a single platform. It provides advanced threat defense, intrusion prevention,   
and protects the network from attacks by monitoring, controlling, and filtering traffic. Key features include:

- Stateful packet inspection  
 - Virtual Private Network (VPN) support  
 - Intrusion Prevention System (IPS)  
 - Web filtering and malware defense  
 - Secure access control and user authentication

# Cisco Catalyst Switches (3850 & 2960)

Cisco Catalyst switches are enterprise-class switches designed for secure   
 and scalable network access.  
 - Cisco Catalyst 3850: Stackable access switches with integrated wireless controller. Supports advanced features   
 like high-performance Layer 3 routing and quality of service (QoS). Supports up to 480 Gbps stacking bandwidth.  
 - Cisco Catalyst 2960: Layer 2 access switch for small to medium networks. Supports basic features like VLANs,   
 STP (Spanning Tree Protocol), and port security. Energy-efficient and simple to deploy for cost-effective LANs.

A black device with many ports

Description automatically generated

A close-up of a white device

Description automatically generated

# DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns IP addresses and other network configuration parameters (like subnet masks and default gateways) to client devices. This reduces the need for manual IP configuration and ensures that devices in a network can communicate efficiently. Key functions include:  
 - Automatic IP assignment  
 - IP address lease management  
 - DNS and gateway configuration

# DNS Server

A Domain Name System (DNS) server resolves human-readable domain names (like www.example.com) into machine-readable IP addresses. This process is essential for web browsing and network operations, as it allows devices to locate and communicate with others over the internet or internal networks. Key functions include:  
 - Domain name resolution  
 - IP address mapping  
 - Caching previous lookups for faster responses

# FTP Server

A File Transfer Protocol (FTP) server enables the transfer of files between a client and a server over a network. FTP is often used for uploading and downloading large files in business environments. Key features include:  
 - File sharing and storage  
 - Authentication and user access control  
 - Data encryption via secure FTP (SFTP)

# WEB Server

A web server hosts and delivers websites or web-based applications to users over the internet or   
 intranet. It processes incoming HTTP/HTTPS requests, interprets them, and sends the appropriate content   
 (web pages, images, scripts). Commonly used web servers include Apache, Nginx, and Microsoft IIS. Key functions include:  
 - Serving static and dynamic content  
 - SSL/TLS encryption for secure connections  
 - Load balancing for high-traffic sites

# Email Server

An email server handles the sending, receiving, and storage of emails. It allows users to communicate   
 using email protocols such as SMTP (Simple Mail Transfer Protocol) for outgoing mail, and IMAP/POP3 for incoming mail.   
 Popular email servers include Microsoft Exchange and Postfix. Key functions include:  
 - Email routing and delivery  
 - Mailbox storage and management  
 - Security features like spam filtering and virus scanning

# VoIP Gateway

A Voice over IP (VoIP) gateway converts voice signals between the public switched telephone network (PSTN) and an IP network. It allows voice calls to be transmitted over IP networks, making it a critical component for enterprises   
 that want to integrate traditional telephony with modern IP-based communication systems. Key features include:  
 - Call routing between IP and analog phones  
 - Codec conversion and compression for voice data  
 - Fax and SMS integration

# Wireless LAN Controller (WLC)

A Wireless LAN Controller (WLC) manages and controls wireless access points in a network, ensuring secure and efficient wireless communication. It centralizes wireless network management, enabling simplified   
 configuration, monitoring, and troubleshooting. Key functions include:  
 - Wireless network security and access control  
 - Centralized configuration for multiple access points  
 - Load balancing and roaming support

# NAS Storage Server

A Network-Attached Storage (NAS) server provides file storage and sharing over a network. It allows users to store and retrieve data from a centralized location, making it ideal for backups, file sharing, and media streaming.   
 NAS servers often come with built-in redundancy and data protection features like RAID. Key functions include:  
 - Centralized file storage and sharing  
 - User access control and permissions  
 - Data redundancy and backups

# IP Addressing

The designated IP address ranges for various network components are as follows:

Management Network: 192.168.10.0/24

WLAN: 10.20.0.0/16

LAN: 172.16.0.0/16

VoIP: 172.30.0.0/16

DMZ: 10.11.11.0/27

Public Addresses:

* - SEACOM: 105.100.50.0/30
* - Safaricom: 197.200.100.0/30

# Technologies Implemented

# Design Tool: Cisco Packet Tracer

Cisco Packet Tracer was used for network design and simulation before the actual deployment.It allowed for a virtual environment to test configurations, create network topologies, and simulate device behavior to ensure functionality before real-world implementation.



# Hierarchical Design

A hierarchical network design model was implemented, consisting of three layers: Core,   
Distribution, and Access. This model improves scalability, redundancy, and network manageability. Redundancy   
is achieved through multiple links between layers to ensure high availability.

# ISPs: Connectivity to an Airtel ISP Router

The network was connected to an Airtel ISP router to provide external internet access. This ensures reliable and high-speed connectivity for the organization's internal network.

# Wireless LAN Controller (WLC)

A close-up of a router

Description automatically generatedEach department was equipped with a Wireless Access Point (WAP) managed by a Wireless LAN   
 Controller (WLC). This provided WiFi access for users and allowed centralized management and monitoring of wireless networks.

# VoIP: Deployment of IP Phones

VoIP (Voice over IP) technology was implemented using IP phones to enable efficient voice   
 communication over the IP network. This solution integrates voice services with the existing data network, reducing costs   
 and simplifying management.

A close-up of a telephone

Description automatically generated

# VLAN: Maintained VLANs with Specific IDs

VLANs (Virtual Local Area Networks) were set up with unique IDs to segregate network traffic.   
VLANs were created for:  
 - Management  
 - LAN (General user traffic)  
 - WLAN (Wireless network traffic)  
 - VoIP (Dedicated for IP phone communication)  
 - Blackhole (For isolating unwanted or suspicious traffic)

# EtherChannel: LACP for Link Aggregation

Link Aggregation Control Protocol (LACP) was used to implement EtherChannel, allowing   
multiple physical links between switches to be combined into a single logical link. This increases bandwidth and provides redundancy in case of link failure.

# Spanning Tree Protocol (STP)

STP was configured to prevent network loops and ensure a loop-free topology. Features like PortFast were enabled on access ports to expedite the connection of end devices, and BPDUguard was applied to prevent the introduction of rogue switches.

# Subnetting: IP Address Allocation

Subnetting was used to logically divide the network into smaller sub-networks. This allows for efficient IP address allocation, improved network management, and enhances security by isolating different departments or services.

# Basic Device Settings

Basic configurations were applied to all network devices, including setting hostnames, enabling secure passwords for access, and configuring necessary logging and monitoring settings to enhance security and manageability.

# Inter-VLAN Routing

Inter-VLAN routing was enabled on multilayer switches to allow communication between different VLANs. This setup ensures that departments can communicate with each other while maintaining network segmentation for security purposes.

# Core Switch: IP Assignment for Multilayer Switches

A black device with many ports

Description automatically generatedMultilayer switches in the core layer were assigned IP addresses to handle both Layer 2 switching and Layer 3 routing. These switches manage both local traffic and inter-VLAN routing.

# DHCP Server: Dynamic IP Allocation

A DHCP server was configured to dynamically assign IP addresses to end devices in the network.This ensures efficient IP management and reduces the chances of IP conflicts.

# HSRP: High Availability Router Protocol

The Hot Standby Router Protocol (HSRP) was implemented to ensure high availability for routing services. In case the primary router fails, the standby router takes over, minimizing downtime.

# Static Addressing: Server Room Devices

Static IP addresses were assigned to critical devices in the server room, such as servers, storage devices, and printers. This ensures stable and predictable access to these resources.

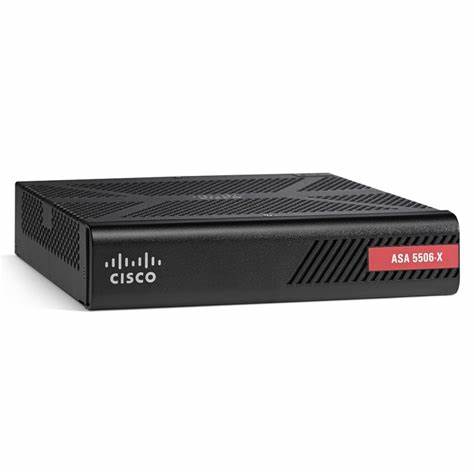
# Routing Protocol: OSPF for Route Advertisement

OSPF (Open Shortest Path First) was selected as the routing protocol to efficiently advertise routes within the internal network. OSPF is a scalable and reliable protocol for dynamic routing, providing fast convergence and optimal path selection.

# Standard ACL for SSH

A Standard Access Control List (ACL) was created to allow secure remote access using SSH. This restricts remote access to specific IP addresses, enhancing security.

# Cisco ASA Firewall

The Cisco ASA firewall was configured to secure the network by controlling incoming and outgoing traffic based on predefined security rules. It provides protection against external threats and ensures internal network segmentation.

Storage and Data Management

# 1. Storage and Data Management

In modern network infrastructure, Storage and Data Management play a critical role in ensuring that organizational data is securely stored, easily accessible, and efficiently managed. For Cytonn Innovation Ltd, a company dealing with cloud-based solutions and an expanding workforce, the importance of robust storage solutions cannot be overstated. With a growing team of 600 staff and departments like ICT, Sales, HR, and Finance, the need to manage large volumes of data, such as business documents, employee information, and financial records, becomes a priority. Below are key elements that define storage and data management in this context:

# 1.1 Data Storage Infrastructure

To meet current and future demands, Cytonn Innovation requires a scalable and redundant data storage system. The company may utilize a hybrid model, incorporating both on-premise storage (within their Data Center or server farm) and cloud storage solutions. This hybrid approach allows the company to leverage the flexibility and scalability of cloud storage while maintaining control over sensitive data by storing it locally. Essential components of storage infrastructure include:

- NAS (Network-Attached Storage): NAS solutions in the DMZ will allow easy access to files and data across departments while maintaining secure access protocols.  
- SAN (Storage Area Networks): A SAN solution could be used to facilitate high-performance block-level storage, especially for mission-critical applications and databases.  
- Cloud Integration: The company will need to seamlessly integrate cloud services (such as AWS, Google Cloud, or Microsoft Azure) to allow remote teams and clients access to data as needed.

# 1.2 Data Security and Redundancy

Data security is paramount, especially given that Cytonn Innovation operates in a global environment with cloud-based services. The company must employ redundancy mechanisms and backups to prevent data loss. Redundancy could be implemented at various levels:

- RAID Configuration: Implementing RAID (Redundant Array of Independent Disks) across storage drives ensures data can be recovered in case of hardware failure.  
- Data Replication: Data replication, either locally or to the cloud, ensures that there are multiple copies of the data available, safeguarding against accidental loss or corruption.  
- Automated Backups: Automated backups to both on-premise servers and cloud-based storage ensure that historical data is preserved, complying with data retention policies and disaster recovery plans.

# 1.3 Data Access and Management Policies

Effective data management requires clear policies on access control and data categorization. Access to sensitive company data, such as customer records or financial information, should be restricted to authorized personnel using role-based access control (RBAC). Additionally, the Active Directory (AD) system will manage user access by authenticating and authorizing users, ensuring that only individuals with proper credentials can access certain data sets.

- Tiered Storage: Data should be categorized based on its importance, where frequently accessed data resides on high-speed storage devices and archival data can be moved to slower, less expensive storage media.  
- Encryption: All sensitive data, both at rest (in storage) and in transit (when being accessed or transferred), should be encrypted to protect against unauthorized access.

# 1.4 Data Recovery and Business Continuity

Cytonn Innovation’s storage and data management system must be designed to support business continuity. In the event of a disaster—such as hardware failure, cyberattacks, or natural disasters—the company needs to recover quickly with minimal data loss. Key measures include:

- Disaster Recovery Plan (DRP): A well-structured DRP that outlines the steps needed to restore critical systems, services, and data.  
- Offsite Backups: Regularly scheduled backups should be stored offsite or in a cloud environment to ensure that a secure copy of the data is available in case of a physical disaster at the main site.  
- Snapshot Technology: Snapshot technology allows for quick backups of the entire system state, providing a fast recovery point to restore data in case of corruption or loss.

# 1.5 Scalability and Future Expansion

Given that Cytonn Innovation is continuously expanding, it is crucial to design a storage system that can scale with the company's growth. The storage infrastructure should support:

- Scalable Cloud Solutions: The company’s cloud storage strategy should be flexible enough to handle an increasing amount of data without requiring substantial upfront investments.  
- Virtualization and Containerization: The use of virtual machines and containers for data storage ensures easy scalability and efficient use of resources.  
- Modular Hardware: On-premise storage systems should use modular hardware that can be easily upgraded by adding more drives or storage shelves as needed.

Device Settings and Configuration

# A group of computer equipment Description automatically generated with medium confidenceDevice Settings and Configuration

Device settings and configuration are critical components in establishing a stable, secure, and efficient network infrastructure. These settings include fundamental configurations like assigning IP addresses, enabling password protection, and setting up protocols that ensure communication and security across the network.

# 1. Basic Device Configuration

Every network device must undergo initial configuration to ensure it can participate in the overall network. Basic settings include:

- Hostname Assignment: Each device is given a unique hostname for easy identification within the network.

- Password Protection: For security, devices are configured with console, enable, and virtual terminal (VTY) passwords. This ensures that only authorized personnel can access or manage the devices.

- Password Encryption: To safeguard the password, the service password-encryption command is applied. This encrypts the stored passwords to prevent unauthorized viewing.

- Banner Messages: A login banner, often containing legal warnings or important network information, is configured to display when users attempt to access the device.

# 2. IP Addressing and Subnetting

IP address configuration is essential for network devices to communicate. Each device, especially switches and routers, is configured with static or dynamic IP addresses:

- Static IPs: Static addresses are assigned to core devices like servers, switches, and firewalls to ensure consistent communication.

- Dynamic IPs (DHCP): For end-user devices and temporary devices like guest systems, Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses.

- Subnetting: Proper subnetting ensures efficient use of the available IP address space and helps to segregate traffic for security and performance optimization.

# 3. Routing Protocols Configuration

Routing protocols are configured to enable devices to communicate across different networks. Open Shortest Path First (OSPF) is often used due to its scalability and efficiency in larger networks. OSPF helps devices learn the network's topology and route traffic efficiently.

- Inter-VLAN Routing: In multi-VLAN setups, multilayer switches are configured to route traffic between VLANs, ensuring communication between different departments or segments.

- Static Routes: Some devices may require static routes, especially in cases where security or performance requires fixed paths for certain types of traffic.

# 4. Security Features

Security settings are essential to prevent unauthorized access and to safeguard network data:

- Access Control Lists (ACLs): ACLs are configured to control which traffic is allowed or denied across different parts of the network.

- SSH Configuration: Secure Shell (SSH) is set up for secure remote access to network devices, ensuring encrypted management sessions.

- Port Security: This feature is often applied on switches to limit the number of devices that can connect to a port, preventing unauthorized device access.

5. Spanning Tree Protocol (STP) Configuration

STP is essential for preventing network loops, which can cause severe disruptions in the network. PortFast and BPDUguard are specific features configured on access ports:

- PortFast: This feature ensures that ports move directly to the forwarding state, reducing downtime for connected devices like computers or phones.

- BPDUguard: This security feature shuts down a port if a bridge protocol data unit (BPDU) is detected, which helps in protecting against rogue switches.

# 6. EtherChannel Configuration

Link Aggregation Control Protocol (LACP) is used for EtherChannel configurations. This combines multiple physical links into a single logical link, improving bandwidth and providing redundancy.

# 7. Testing and Verification

After configuring devices, testing is crucial to ensure that settings are correct and that devices can communicate as expected. This includes:

- Ping Tests: Testing connectivity between devices using ICMP ping.

- Traceroute: Verifying the path packets between devices.

- Show Commands: Various show commands are used to inspect the configuration and status of interfaces, protocols, and routing tables.

Effective device settings and configurations form the backbone of any network. They ensure smooth operation, security, and optimal performance, allowing the organization to focus on its core business needs.

**Future Expansion in Network Design**

Future expansion is a critical consideration in network design, particularly for organizations that anticipate growth or changes in their operational requirements. Proper planning for future expansion ensures that the network can accommodate increased demand without requiring a complete overhaul, which can be costly and disruptive. Below are key aspects to consider when planning for future expansion in a network infrastructure:

# 1. Scalability

Scalability refers to the ability of the network to handle increased loads by adding resources rather than replacing existing infrastructure. A scalable network is designed with the following elements:

- Modular Hardware: Use of modular switches and routers that can be upgraded or expanded with additional modules as needed. This allows for increased capacity without the need to replace entire devices.

- Virtualization: Implementing virtualized servers and network functions allows for easy scaling. Virtual machines can be added or adjusted based on the workload, providing flexibility and efficient resource management.

- Cloud Integration: Utilizing cloud services can provide additional resources on-demand, allowing the organization to scale up or down based on current needs without significant capital investment.

# 2. IP Addressing Scheme

A well-planned IP addressing scheme is essential for accommodating future growth. Considerations include:

- Subnets: Implementing a subnetting strategy that allocates enough IP address space for future devices. For instance, using larger subnets can allow for easier addition of devices without the need for immediate readdressing.

- Dynamic IP Allocation**:** Utilizing DHCP for dynamic IP address allocation can simplify the process of integrating new devices into the network, as they will automatically receive an appropriate IP address without manual configuration.

# 3. Network Redundancy

To ensure continuity and reliability during expansion, it’s important to have redundancy built into the network design. This includes:

- Redundant Links: Establishing multiple network paths can prevent downtime if one link fails. Technologies such as Link Aggregation Control Protocol (LACP) can be used to combine multiple physical links into a single logical link for redundancy.

- Failover Solutions: Implementing failover systems, such as Hot Standby Router Protocol (HSRP), ensures that if one device fails, another can take over seamlessly, minimizing disruptions during expansion.

# 4. Future-proofing Technologies

Choosing technologies that are adaptable and compatible can save time and resources during future expansions:

- Next-Generation Equipment: Invest in next-generation network equipment that supports emerging technologies, such as Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), which can simplify management and increase flexibility.

- Emerging Standards: Stay updated on emerging standards and protocols to ensure compatibility with new devices and technologies, minimizing integration challenges in the future.

# 5. Capacity Planning

Capacity planning involves forecasting future network demands and ensuring that the infrastructure can meet those needs. This includes:

- Traffic Analysis: Regularly analyze network traffic patterns to anticipate growth areas. This analysis can inform decisions on hardware upgrades, bandwidth requirements, and the need for additional services.

- User Needs Assessment: Engage with different departments to understand their future needs. This information can guide decisions on resource allocation, such as storage, computing power, and network services.

# 6. Documentation and Policies

Maintaining thorough documentation and clear policies can facilitate future expansions by providing guidelines and a roadmap:

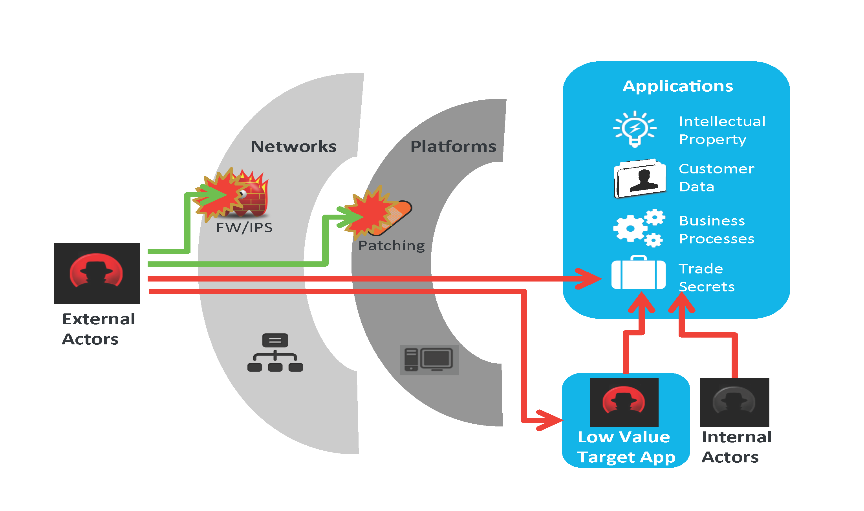
- Network Documentation: Keeping detailed records of the network architecture, configurations, and IP addressing schemes helps streamline future modifications and expansions.

- Change Management Policies: Establishing change management policies ensure that any changes to the network are systematically planned, reviewed, and executed, minimizing risks during expansion.

# Conclusion

Planning for future expansion in network design is essential for ensuring that an organization can grow and adapt to changing needs without significant disruptions. By incorporating scalability, redundancy, capacity planning, and the use of adaptable technologies, organizations can create a resilient network infrastructure that supports their long-term goals. As Cytonn Innovation Ltd prepares to move into a new building, these considerations will play a pivotal role in ensuring the network can effectively support its ongoing growth and evolution.

application security

Application security, or app sec, is the practice of using security software, hardware, techniques, best practices, and procedures to protect computer applications from external [security threats](https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams).

Security was once an afterthought in software design. Today, it's an increasingly critical concern for every aspect of application development, from planning through deployment and beyond. The volume of applications developed, distributed, used and [patched](https://www.techtarget.com/searchenterprisedesktop/definition/patch) over networks is rapidly expanding. As a result, application security practices must address an increasing variety of threats.

# How does application security work?

Security measures include improving security practices in the [software development lifecycle](https://www.techtarget.com/searchsoftwarequality/definition/software-development-life-cycle-SDLC) and throughout the application lifecycle. All app sec activities should minimize the likelihood that malicious actors can gain unauthorized access to systems, applications or data. The ultimate goal of application security is to prevent attackers from accessing, modifying or deleting sensitive or [proprietary](https://www.techtarget.com/whatis/definition/proprietary) data.

Any action taken to ensure application security is a countermeasure or security control. The National Institute of Standards and Technology ([NIST](https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework)) defines a security control as: "A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements."

An [application firewall](https://www.techtarget.com/searchsoftwarequality/definition/application-firewall) is a countermeasure commonly used for software. Firewalls determine how files are executed and how data is handled based on the specific installed program. [Routers](https://www.techtarget.com/searchnetworking/definition/router) are the most common countermeasure for hardware. They prevent the [Internet Protocol (IP) address](https://www.techtarget.com/whatis/definition/IP-address) of an individual computer from being directly visible on the Internet.

# Why is application security important?

Application security -- including the monitoring and [managing of application vulnerabilities](https://www.techtarget.com/searchsecurity/tip/Five-common-Web-application-vulnerabilities-and-how-to-avoid-them) -- is important for several reasons, including the following:

Finding and fixing vulnerabilities reduces security risks and doing so helps reduce an organization's overall [attack surface](https://www.techtarget.com/whatis/definition/attack-surface).

Software vulnerabilities are common. While not all of them are serious, even noncritical vulnerabilities can be combined for use in attack chains. Reducing the number of security vulnerabilities and weaknesses helps reduce the overall impact of attacks.

Taking a proactive approach to application security is better than reactive security measures. Being proactive enables defenders to identify and neutralize attacks earlier, sometimes before any damage is done.

As enterprises move more of their data, code and operations into the cloud, attacks against those assets can increase. Application security measures can help reduce the impact of such attacks.

# Application security services

Securely build, deploy and iterate applications everywhere by transforming DevOps into Develops including people, processes and tooling.



# Overview

Cloud migration, microservices and container adoption are driving application modernization, but are your applications secure? Application vulnerabilities are often uncovered late because DevOps and security processes can be disjointed. Application security services professionals with a deep understanding of the software development lifecycle (SDLC) can help assess and transform your “shift-left” and DevSecOps practices.

# Benefits

-Unify people, processes and technology

Plans, designs, implements, integrate and deploy security strategically into every step of the development lifecycle. Shared skills sets and collaboration help transform people, process and technology into DevSecOps best practices, backed up by the IBM® Application Security Center of Excellence.

-Increases quality, regulatory compliance, and cost reduction

Empowers “shift-left” practices to reduce app security defects early in the SDLC. This helps reduce the cost of fixing software vulnerabilities and improve compliance with industry and government regulations.

-Securely accelerates development and innovation

Enables security automation and integration into the continuous integration and continuous deployment pipeline. Application security training onsite or online can drive productivity between DevOps and security for rapid innovation and security-focused software development.

# Capabilities

Application security services are focused on three key areas of DevSecops, training and threat modeling. DevSecOps services help development, security and operations teams share skills for greater collaboration. Either onsite or digital application security training builds and strengthens the skills and expertise to build and run enterprise-grade software. Lastly, application threat modeling services provide an in-depth analysis of application security vulnerabilities.

# Common application security weaknesses and threats.

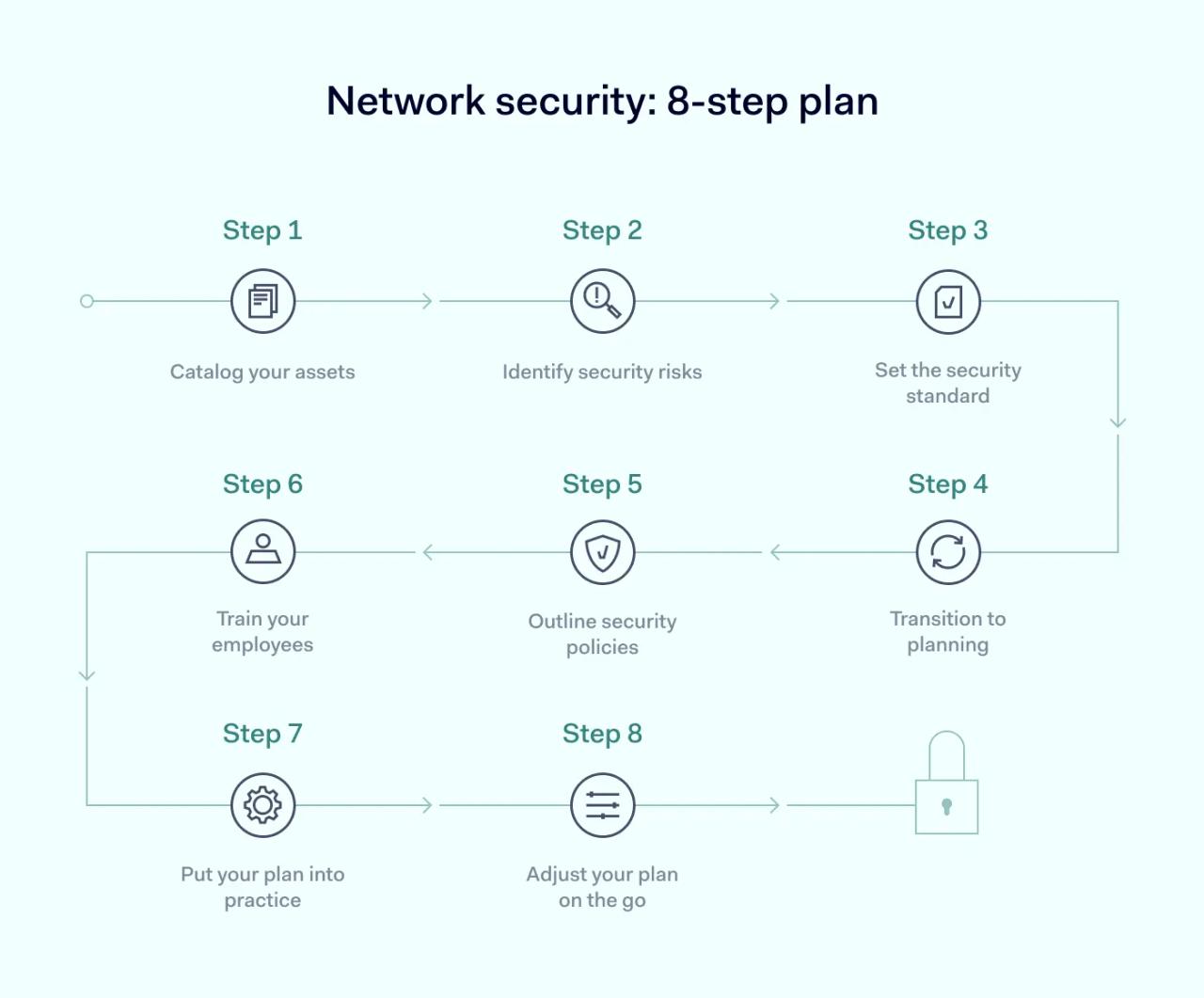
The most common application security weaknesses are well-known. Various organizations track them over time. The Open Web Application Security Project ([OWASP](https://www.techtarget.com/searchsoftwarequality/definition/OWASP)) Top Ten list and the Common Weakness Enumeration ([CWE](https://www.techtarget.com/searchsecurity/definition/Common-Weakness-Enumeration)) compiled by the information security community are two of the best-known lists of application weaknesses.

The OWASP list focuses on web application software. The CWE list focuses on specific issues that can occur in any software context. Its goal is to provide developers with usable guidance on how to secure their code.

# How is network security implemented?

T

o begin network security implementation actions on your end, it's useful to look at the matter overall.

Here's an example of how a security professional could approach security model adaptation in a company.

# 1. Catalog your assets

The first step should be to **catalog all the organization's assets connected to the internet**. It will shed light on the scope of the protection that needs to be introduced and will help to shape your [network security strategy](https://nordlayer.com/learn/network-security/what-is-network-security/).

The list should include all devices ranging from servers to employees' laptops — anything that stores business data. The devices that store the most sensitive data types should be best secured. However, don't forget to check which devices pass data over what networks. This may reveal weak spots in your infrastructure.

forget to check which devices pass data over what networks. This may reveal weak spots in your infrastructure.

## 2. Identify security risks

Each asset that you've identified is susceptible to various security risks. However, some risks are very severe and require immediate solutions, while others may be more hypothetical. The key to this part is **identifying the most likely and the most dangerous risks.**

An example of such a risk could be a data breach due to unencrypted communication channels or an insider threat that could leak company data externally. Remember that risk assessment shouldn't be done once and forgotten — it should be a routine process as your business develops.

## 3. Set the security standard

Once you know what assets you're using and what risks are the most likely, it's time to **evaluate what security requirements you should set up**. Some budgeting options should also come into play as, depending on the area, it may prove easier or harder to secure, which can affect its final price tag.

You may also run into some limitations like legacy hardware, which means that in some cases, the only possibility to avoid risks would be to replace some legacy systems altogether. However, as a rule of thumb, try to set a total budget and plan to fit it.

## 4. Transition to planning

If you've completed the first three steps, you have all you need to **develop your security plan.** The assets have to be secured in such a way as to eliminate identified risks using various methods within a set budget.

The plan should detail how various assets will be secured and how the new solutions or approaches directly help address network flaws are found. This part should also be transitioned into an implementation strategy that could be converted into tasks that the technical employees should implement.

## 5. Outline security policies

Up to this point, your network security plan focused on the technical parts. What you shouldn't forget is that you should **raise security standards for your employees**, as well as your assets. At the most rudimentary level, it should include various guidelines each employee should follow when accessing work resources.

Outline the acceptable and unacceptable use cases of network assets. In addition, detail how various access permissions will be assigned. This will help ensure that the employees aren't exposed to the full network data set, which helps to ensure its security.

## 6. Train your employees

Regarding employees, it's not enough to set rules and everyone expects to know how to apply them in practice. Even if your employee network security guidelines are basic, you should still **conduct company-wide training**. Conducting compliance training to ensure employees understand what's at stake and what's expected of them is not a bad idea.

Your IT personnel will also require training, which should be more in-depth. As they will be directly ensuring the maintenance of the system, IT staff should be qualified to use and resolve any errors that will arise from the new systems.

## 7. Put your plan into practice

Finally, **the strategy you've come up with should be implemented**. To have a smooth transition, you should put your plan in a timeline — note all outsourcing requirements you'll need and identify which improvements will require how many person-hours.

This is also a good step to evaluate how many contingencies you could expect. This should be reflected in your plan, as the trickier improvements should have some room for time. This will help to move forward with the implementation actions and not get delayed far behind.

## 8. Adjust your plan on the go

The last note should be that your network security plan's work doesn't end with its implementation. You should **continuously monitor and evaluate its performance to see what could be improved or altered**. As the risk landscape changes, this should shape your network security plan. However, the adjustments should be made the same way the plan was implemented.

The Roles and Responsibilities

A secure company network system is crucial for protecting sensitive data, ensuring operational continuity, and maintaining trust with clients and partners. Here are the key roles and responsibilities associated with such a system:

## 1. Network Security Administration

**Monitor Network Traffic**: Continuously observe and analyze network activity for unusual behavior or potential threats.

**Implement Security Protocols**: Establish and enforce security policies, firewalls, and intrusion detection systems.

**Manage User Access**: Control user permissions and access levels to sensitive information based on roles.

## 2. Data Protection

**Encrypt Sensitive Data**: Use encryption methods for data in transit and at rest to prevent unauthorized access.

**Regular Backups**: Ensure regular backups of critical data and implement disaster recovery plans.

## 3. Incident Response

**Develop an Incident Response Plan**: Create and maintain procedures for responding to security breaches or threats.

**Conduct Investigations**: Analyze incidents to understand their causes and prevent future occurrences.

## 4. Compliance and Auditing

**Adhere to Regulations**: Ensure compliance with relevant laws and industry standards (e.g., GDPR, HIPAA).

**Conduct Security Audits**: Regularly evaluate security measures and policies for effectiveness and compliance.

## 5. User Education and Training

**Train Employees**: Provide security awareness training to employees to recognize phishing and other social engineering attacks.

**Promote Best Practices**: Encourage the use of strong passwords, secure browsing habits, and report suspicious activities.

## 6. Physical Security

**Secure Hardware**: Protect physical assets such as servers and workstations with locks, surveillance, and controlled access.

**Monitor Physical Access**: Ensure only authorized personnel have access to critical network infrastructure.

## 7. Vulnerability Management

**Regular Updates and Patching**: Keep software and systems up to date to protect against known vulnerabilities.

**Conduct Penetration Testing**: Regularly test the network for vulnerabilities and address any identified weaknesses.

## 8. Network Architecture Design

**Segment Network**: Use network segmentation to limit access and contain potential breaches.

**Implement Redundancy**: Design networks for resilience with redundant systems to ensure availability.

## 9. Collaboration with IT and Management

**Communication Risks**: Regularly report security status and risks to management.

**Collaborate on Policies**: Work with IT teams to develop comprehensive security policies and strategies.

## 10. Emerging Threat Awareness

**Stay Informed**: Keep up with the latest security threats and trends to adapt strategies accordingly.

**Utilize Threat Intelligence**: Implement threat intelligence solutions to anticipate and mitigate potential risks

# Final Testing: Communication Verification

## After configuring the entire network, thorough testing was conducted to ensure proper communication between all devices and verify that all configurations were applied correctly. This testing included end-to-end connectivity checks, security audits, and performance evaluations.

# Conclusion

The design and implementation of a secure network system for Cytonn Innovation Ltd is critical to ensuring operational efficiency and safeguarding sensitive data. By employing a structured approach with robust security measures, the new network will support the company's growth and adaptability in the digital landscape.

# A computer server room with a cloud of information Description automatically generated with medium confidenceReferences

1. Cisco Systems, "Cisco ASA 5500-X Series Firewalls", Cisco Official Documentation.  
2. Microsoft, "Azure Cloud Services Overview", Microsoft Azure Documentation.  
3. Amazon Web Services, "AWS Storage Solutions", AWS Official Documentation.  
4. Google Cloud, "Cloud Storage for Business", Google Cloud Documentation.

5. reach out on [GitHub](https://github.com/MuhammedShehta/SECURE-COMPANY-PROJECT1-DEPI-OCT2024)