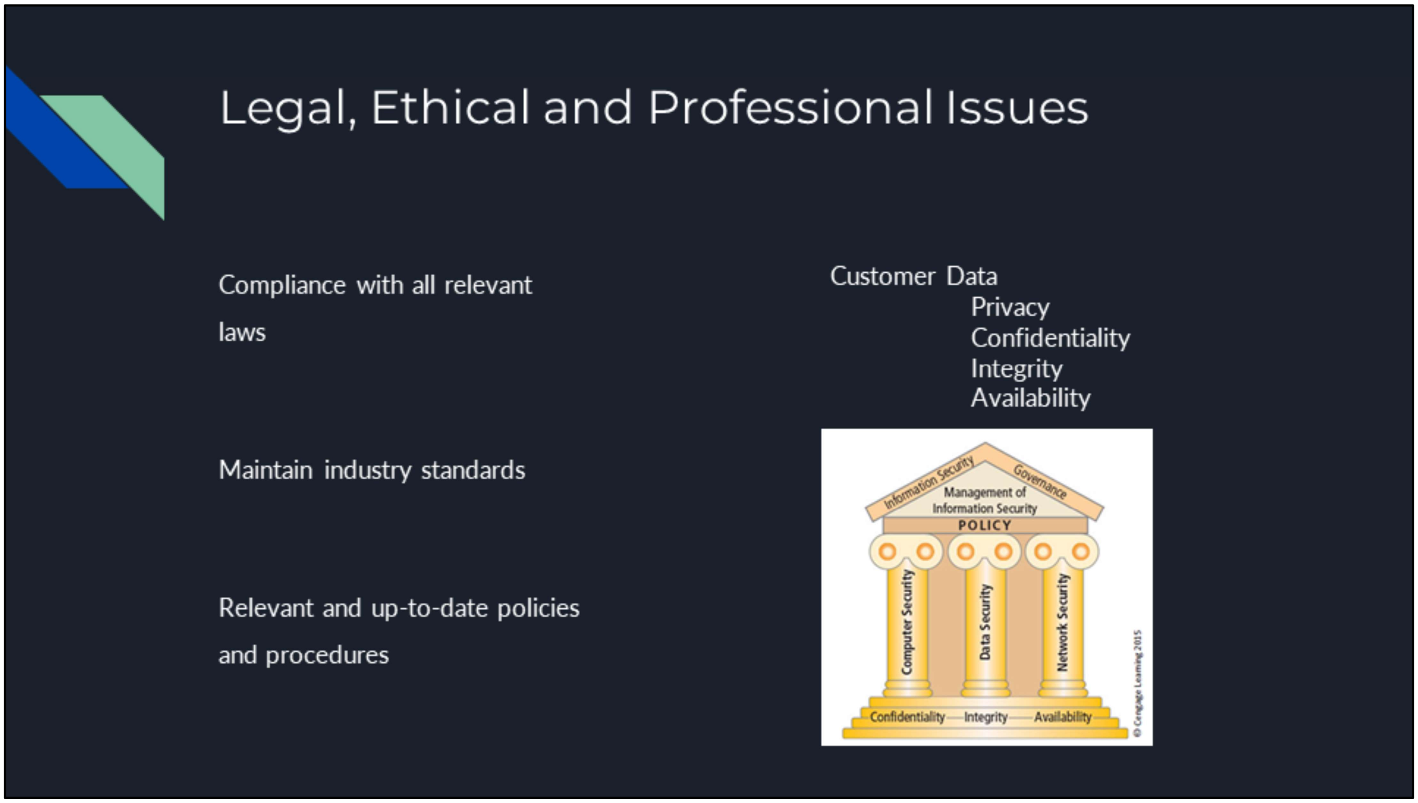
Security Program Implementation Plan

Nicholas Jacob & Tyler Martinez
University of Advancing Technology

April 17, 2022



Legal, Ethical and Professional Issues

Compliance with all relevant laws

Maintain industry standards

Relevant and up-to-date policies and procedures

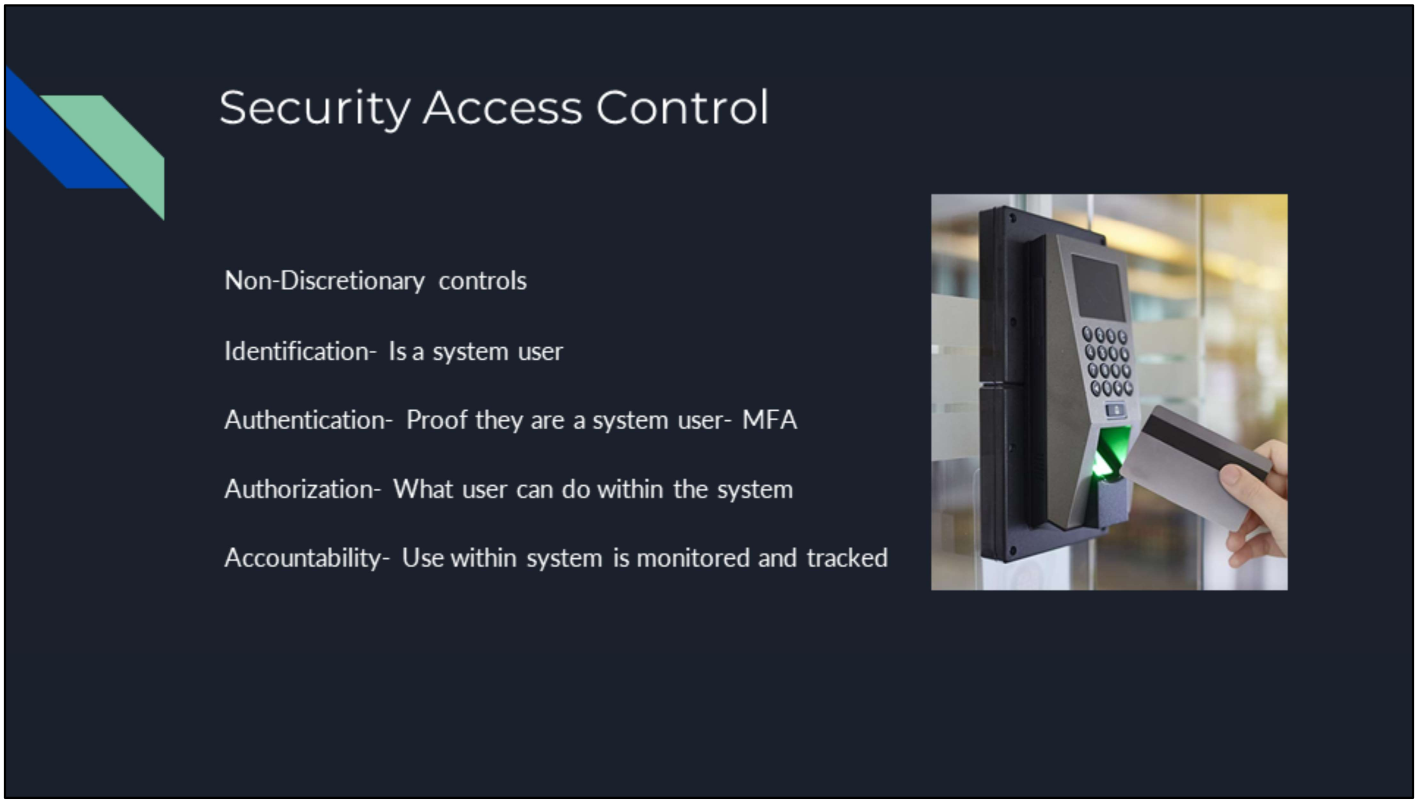
Customer Data
- Privacy
- Confidentiality
- Integrity
- Availability

Information Security
Governance
Management of Information Security
POLICY
Computer Security
Data Security
Network Security
Confidentiality
Integrity
Availability
© Cengage Learning 2015

Company is being compliant with all laws ie HIPAA (Health Insurance Portability and Accountability Act), FTCA (Federal Trade Commission Act), Federal Privacy Act, FOIA (Freedom of Information Act

Standards ie ISO 27001, ISO 20000-1 and others from organizations like ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology)

Policies and Procedures carried over from existing data centers will be enforced. Trainings will be conducted



Security Access Control

Non-Discretionary controls

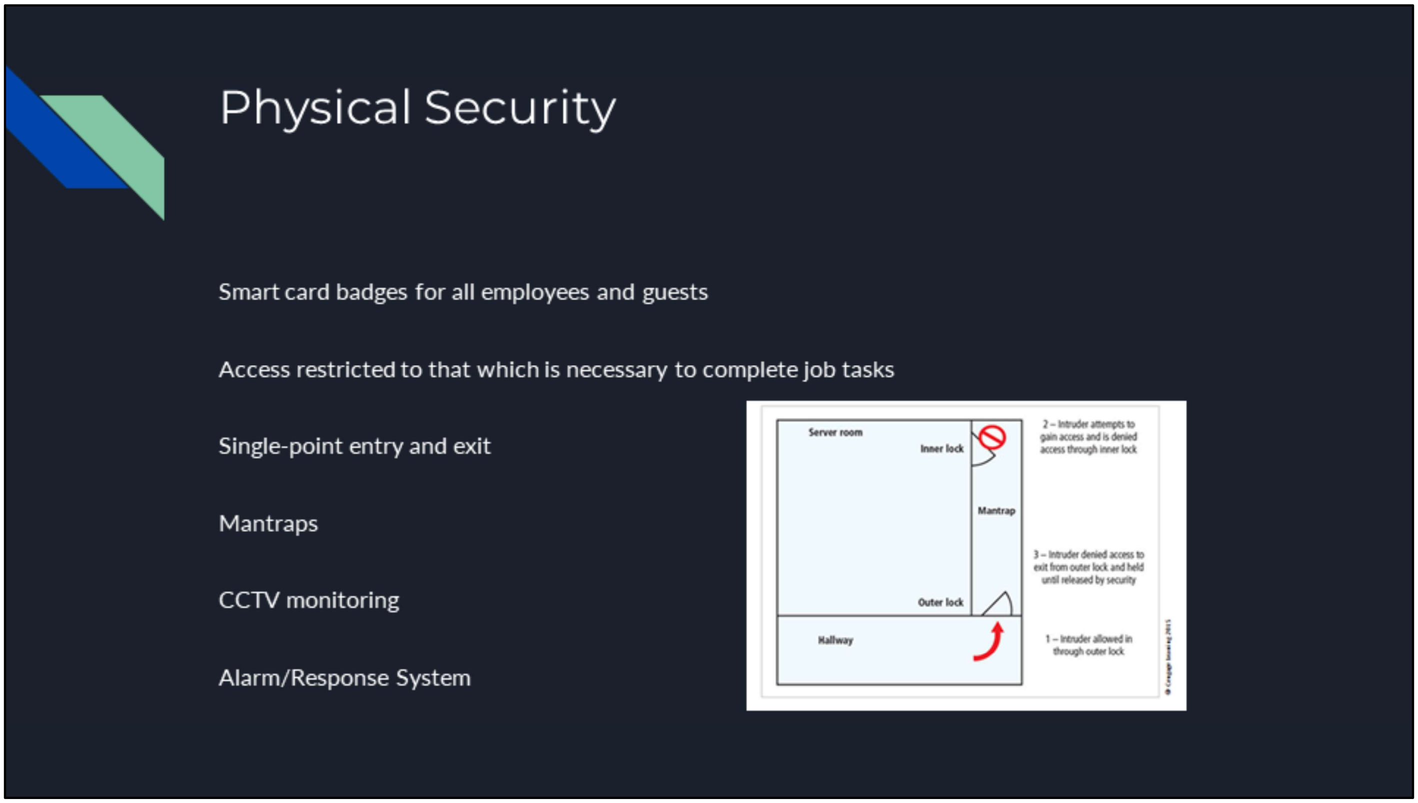
Identification- Is a system user

Authentication- Proof they are a system user- MFA

Authorization- What user can do within the system

Accountability- Use within system is monitored and tracked

Access control given by a central authority- the company management decides access to data only necessary for job tasks to be complete
Identification- Smart Card badges help employee say who they are
Authentication- Pin number and biometrics (fingerprint) provided per access request that must match the employee info of the badge; scrambled numbers when typing pin to prevent pattern mirrors
Authorization- Authenticated employees are given access to “authorized” data authorization given per person or “project” group
Accountability- logs are created and stored for “reasonable” amount of time for auditing or incident response



Physical Security

Smart card badges for all employees and guests

Access restricted to that which is necessary to complete job tasks

Single-point entry and exit

Mantraps

CCTV monitoring

Alarm/Response System

Server room
Inner lock
2 – Intruder attempts to gain access and is denied access through inner lock
Mantrap
3 – Intruder denied access to exit from outer lock and held until released by security
Outer lock
Hallway
1 – Intruder allowed in through outer lock
© Cengage Learning 2015

All personnel will be issued smart card badges that show level of access and that act as their credentials. Smart cards will hold employee's certificates required for gaining access to their required parts of the building as well as for logging into terminals and other devices.

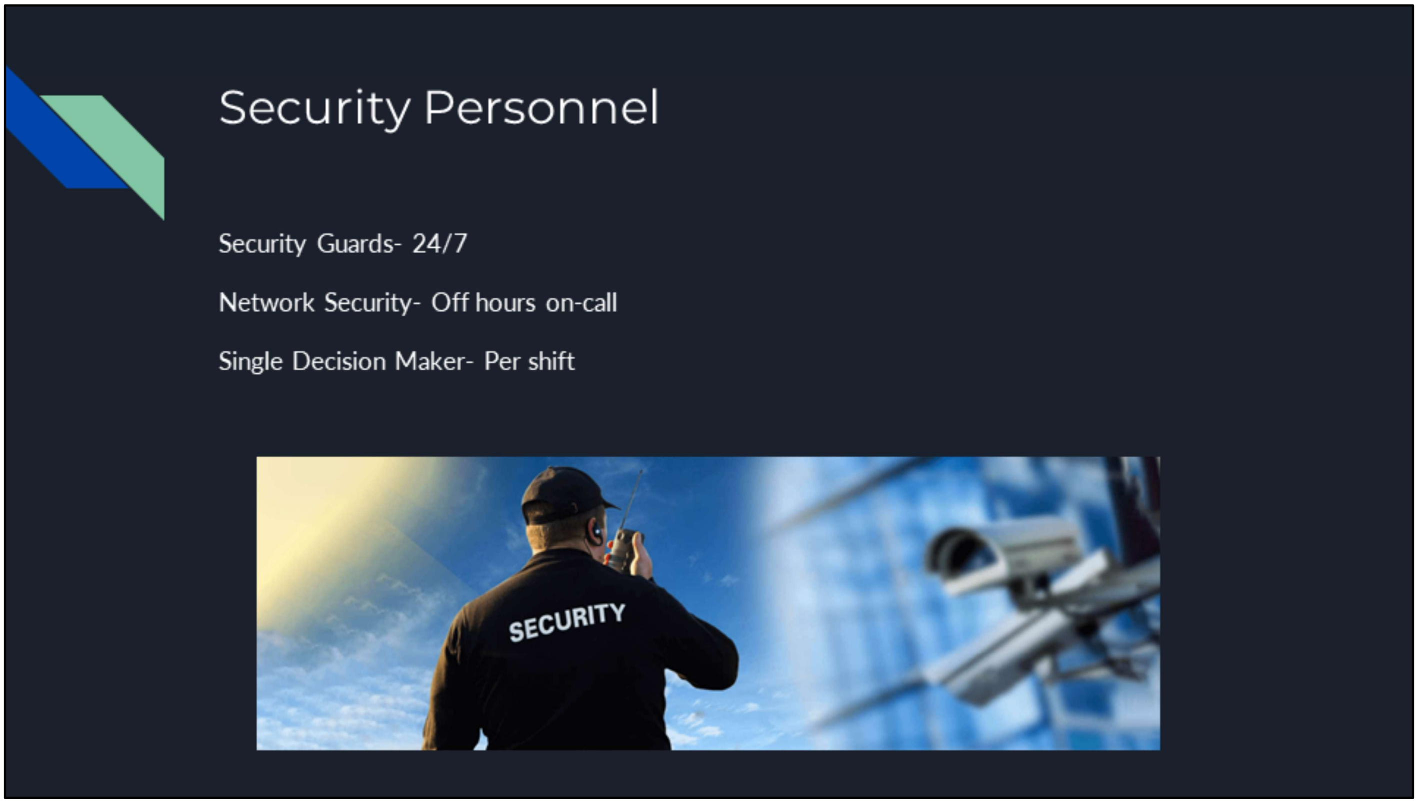
Personnel will only have access to parts of the building and parts of the network required for doing their job.

Personnel will enter and exit through the front of the building except for during emergency situations. Entrances to the building as well as specified restricted areas will have mantraps in place to prevent tailgating of unauthorized individuals.

Mantraps in high-security areas to prevent tailgating

A closed network of cameras will be present and monitored by 24 hour security personnel.

Systems for detecting fire/smoke, intrusion, or other environmental disturbances; response to detections ie fire suppression, environmental controls



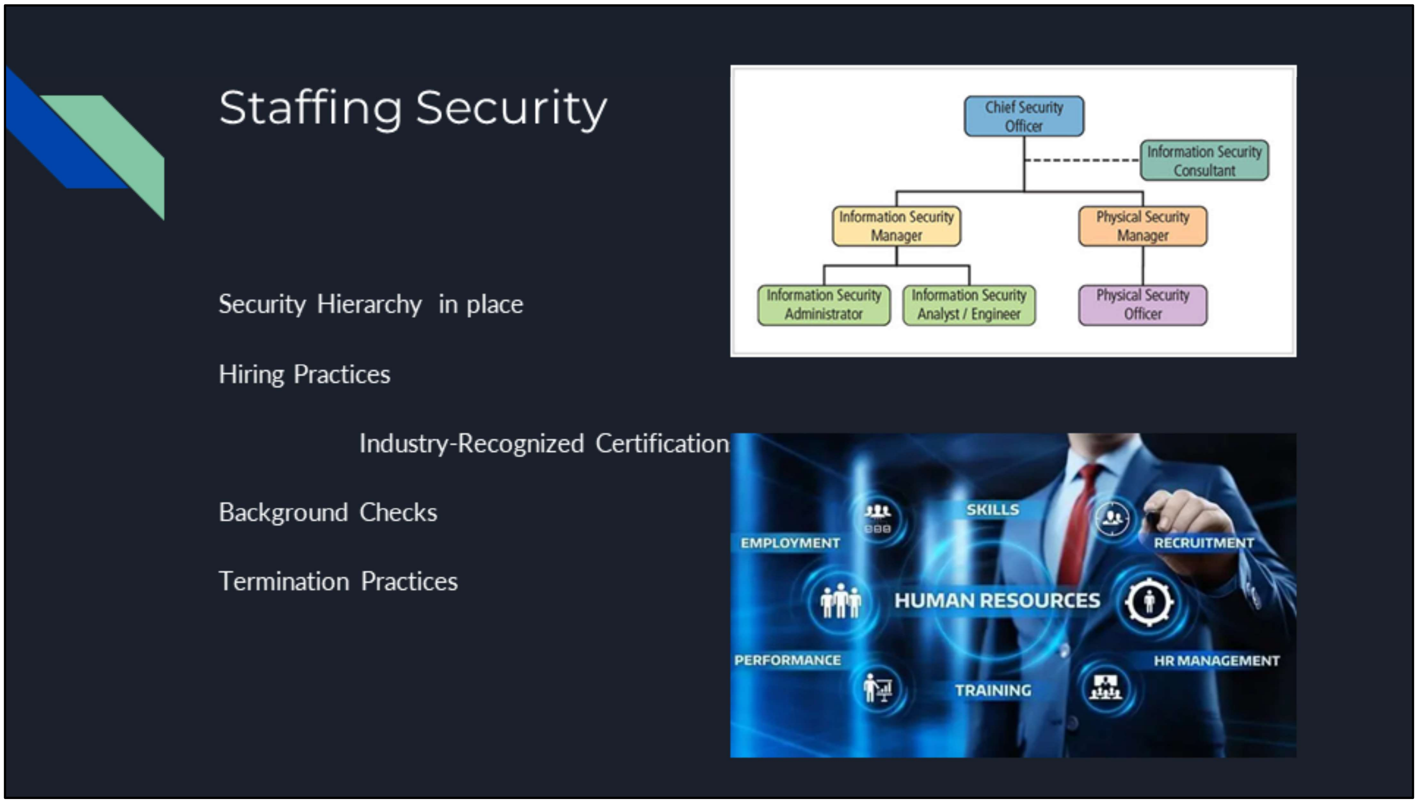
Security Personnel

Security Guards- 24/7

Network Security- Off hours on-call

Single Decision Maker- Per shift

Security Guards- job is physical security enforcement and monitoring- hiring preference on veterans or prior law enforcement
Net Sec- Certified personnel whose primary job is to ensure the security of the network
Decision Maker- In the case of emergency or time sensitive incident a single "manager" level person is the designated decision maker for the shift. This person makes the final decision when time is an important factor or multiple choices are brought forth. Avoid too many Chiefs not enough Indians



Staffing Security

Security Hierarchy in place

Hiring Practices

Industry-Recognized Certification

Background Checks

Termination Practices

Chief Security Officer
Information Security Consultant
Information Security Manager
Physical Security Manager
Information Security Administrator
Information Security Analyst / Engineer
Physical Security Officer
SKILLS
EMPLOYMENT
RECRUITMENT
HUMAN RESOURCES
PERFORMANCE
HR MANAGEMENT
TRAINING

Hierarchy to establish who has final say on important security matters

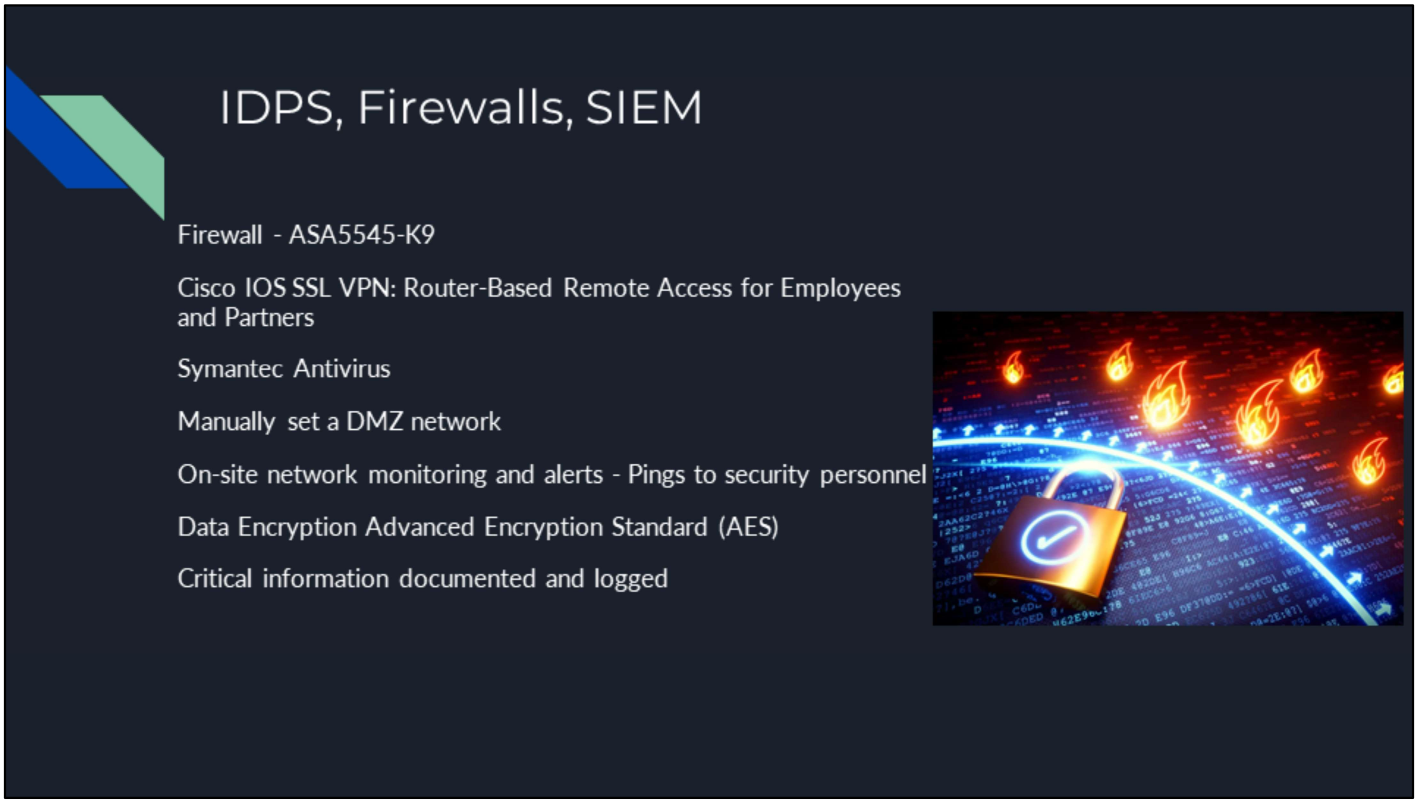
Verify qualifications and position requirements are met

Certifications/experience related to position

Background checks to look for possible vulnerabilities for blackmail or risk of other financial liabilities

Termination- (non-friendly) remove all access before termination to prevent retaliation, all badges, keys, company property returned, employee escorted out with all belongings

Termination- (friendly) resignation, retirement, promotion, transfer/relocation: notified in advance, positive security maintained, expiration date set on access, logs audited for possible breach upon departure



IDPS, Firewalls, SIEM

Firewall - ASA5545-K9

Cisco IOS SSL VPN: Router-Based Remote Access for Employees and Partners

Symantec Antivirus

Manually set a DMZ network

On-site network monitoring and alerts - Pings to security personnel

Data Encryption Advanced Encryption Standard (AES)

Critical information documented and logged

Cisco ASA 5545-X Adaptive Security Appliance

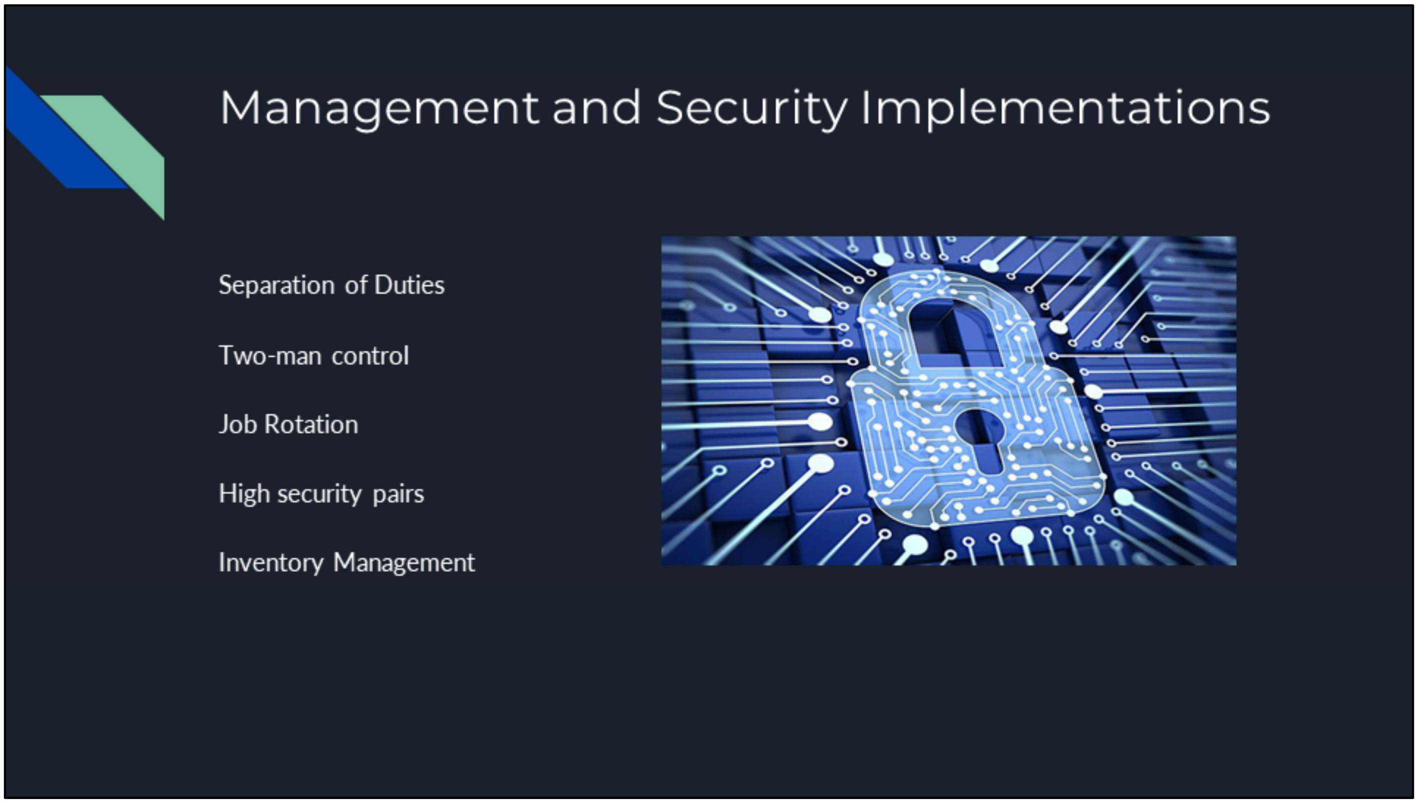
Advanced, enterprise-wide virus protection and monitoring from a single management console

Symantec tamper protection guard against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures

Integrated Web-based graphical reporting:

Scalability to support thousands of users

(shut down outside access while maintaining internal network)(external router)



Management and Security Implementations

Separation of Duties

Two-man control

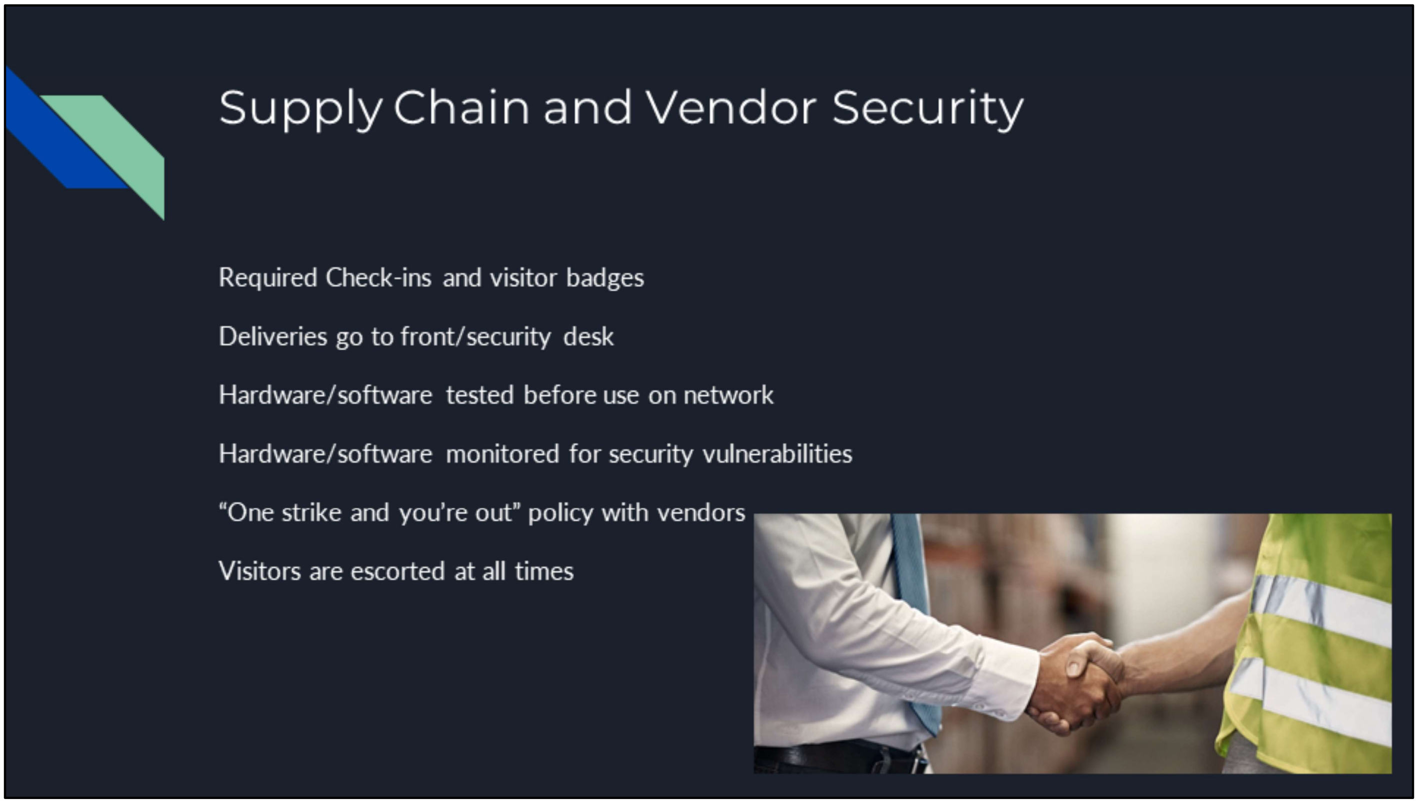
Job Rotation

High security pairs

Inventory Management

Good practice for preventing information security violations and giving temporary additional access to individuals.
Two individuals review and approve each other's work before the task is categorized as finished.
Ensure employees know each other's jobs. Eliminates single-points of failure with personnel in case an employee leaves or is unexpectedly absent
Access to high security areas such as server room will require 2 employees present and in eye sight at all times
Equipment is inventoried and inspected monthly, classified information also inventoried

No unlogged/uninventoried equipment checked out to employees



Supply Chain and Vendor Security

Required Check-ins and visitor badges

Deliveries go to front/security desk

Hardware/software tested before use on network

Hardware/software monitored for security vulnerabilities

“One strike and you’re out” policy with vendors

Visitors are escorted at all times

Required check-in for all people and visitor badges with temp credentials ie janitors or large deliveries
Purchased hardware and software to be tested in a closed network for testing before being put on the company network. This is to check for counterfeit or embedded malware.
3rd party hardware/software monitored for security patches and firmware updates in case of vulnerabilities
Counterfeit or tampered with vendor products don’t get second chance

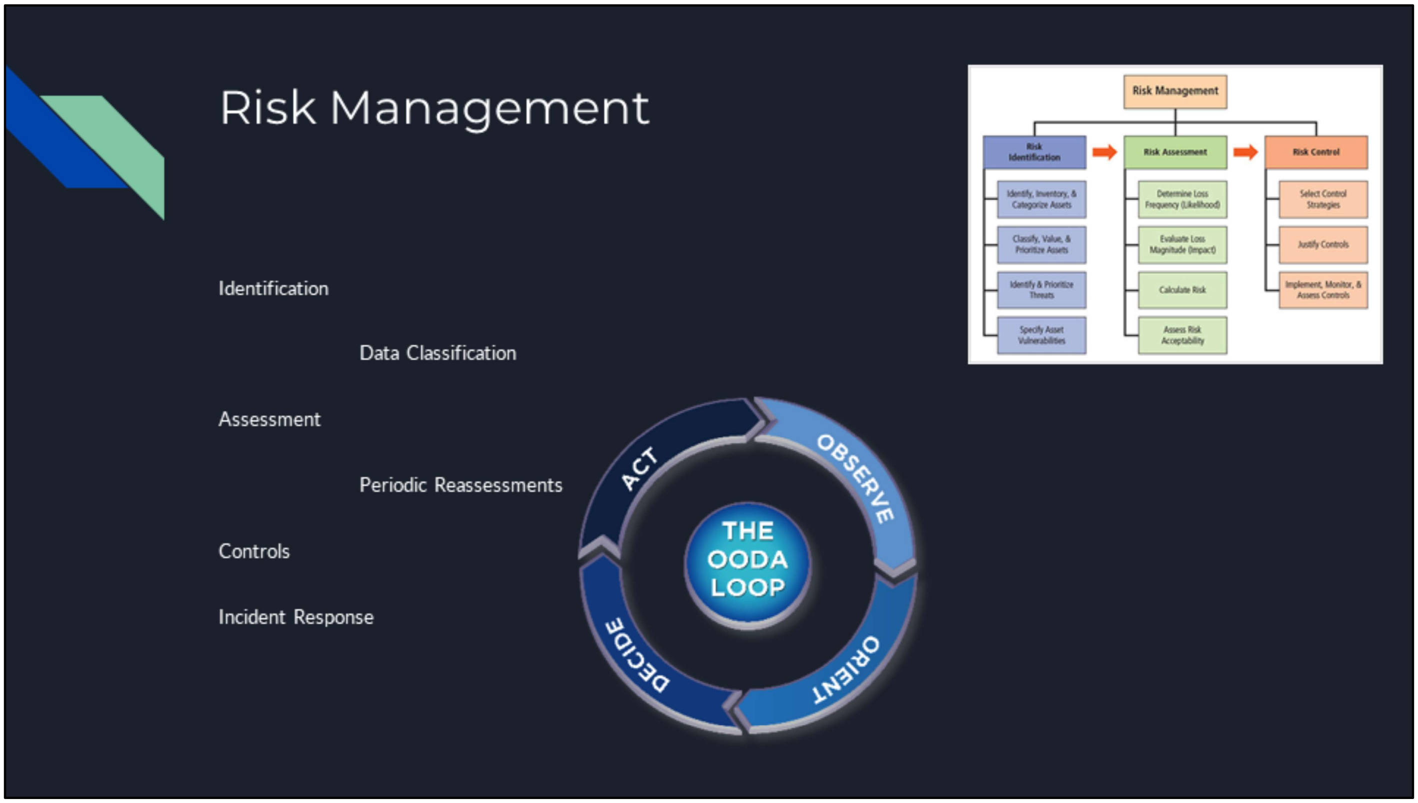
Security Operations Maintenance

Routine Penetration testing

3rd party penetration testing (semi-annually)

Trainings and Drills

This is where we we have an in house testing of the different types of vulnerabilities that could be possible
We will also conduct 3rd Party testing, where we hire an outside source to come determine what we could improve upon if anything. This will be held every six months, but not along the in house testing. This means there will be testing done every three months. It will consist of in-house testing, followed by the 3rd party testing three months later. Then the cycle will continue.
We will issue constant training guides to help protect our employees from potential phishing schemes.This training will be included when we onboard a new employee as well. Scheduled and surprise drills will be conducted for scenarios such as fire or active shooter



Risk Management

Identification

Data Classification

Assessment

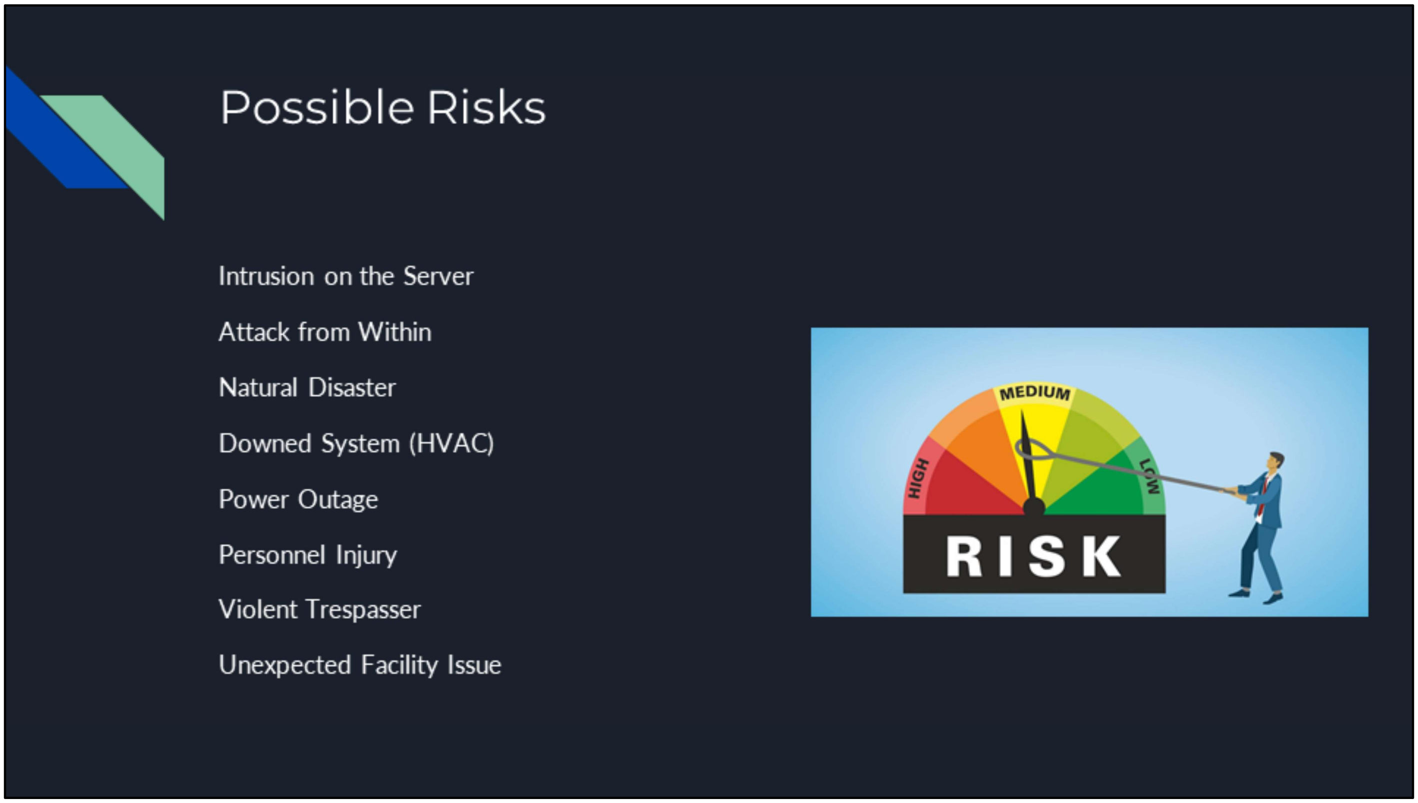
Periodic Reassessments

Controls

Incident Response

Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Determine Loss Frequency (Likelihood)
Evaluate Loss Magnitude (Impact)
Calculate Risk
Assess Risk Acceptability
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls
THE OODA LOOP
OBSERVE
ORIENT
DECIDE
ACT

Data should be given a classification and value level to help assign a level of risk it presents
Risk management is a constant endeavour, new risks should be looked and planned for constantly
Once identified risks are assessed, relevant control measures should be put in place to prevent or mitigate
Personnel should be assigned and know what their role is in case of an incident



Possible Risks

Intrusion on the Server

Attack from Within

Natural Disaster

Downed System (HVAC)

Power Outage

Personnel Injury

Violent Trespasser

Unexpected Facility Issue

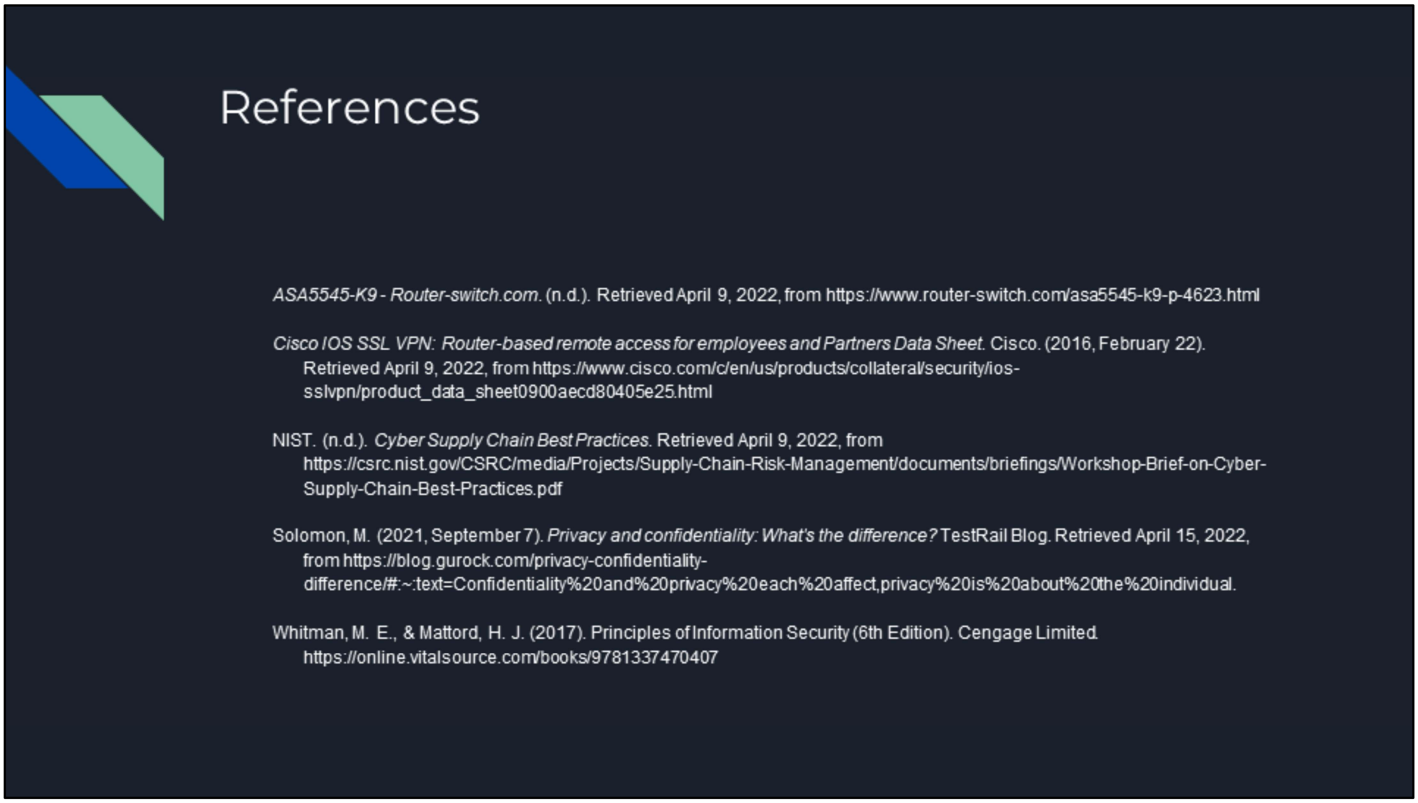
HIGH
MEDIUM
LOW
RISK

Primary Solution, keep data on a secure backup server off base.

Attacks from within, no one person can be alone while in the more sensitive and secure areas of the base.

During a natural disaster the information that can be transferred before the hit will be sent over. If there is no time for a backup, there is always the off base server that contains the essential to run files for the company.

Busted water pipe



References

ASA5545-K9 - Router-switch.com. (n.d.). Retrieved April 9, 2022, from https://www.router-switch.com/asa5545-k9-p-4623.html

Cisco IOS SSL VPN: Router-based remote access for employees and Partners Data Sheet. Cisco. (2016, February 22). Retrieved April 9, 2022, from https://www.cisco.com/c/en/us/products/collateral/security/ios-sslvpn/product_data_sheet0900aecd80405e25.html

NIST. (n.d.). *Cyber Supply Chain Best Practices*. Retrieved April 9, 2022, from https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

Solomon, M. (2021, September 7). *Privacy and confidentiality: What's the difference?* TestRail Blog. Retrieved April 15, 2022, from https://blog.gurock.com/privacy-confidentiality-difference/#:~:text=Confidentiality%20and%20privacy%20each%20affect,privacy%20is%20about%20the%20individual.

Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security (6th Edition). Cengage Limited. https://online.vitalsource.com/books/9781337470407