Designing a Secure Network for the Strome College of Business

Matthew Chewning, Christopher Hossele, and Jaden Howell

IT417

Dr. Kalburgi

December 2, 2024

Contribution

Christopher Hossele - Host Hardening with Update Policies and Implementation, Application and Software Security Policies, Data Protection Measures, Data Protection Technology, Backup Locations, Recovery Measures

Matthew Chewning - Introduction, Mission Statement, Network Setup, Network Diagram, Threats and Attacks, Planning, Organization, Risk Analysis, Threat-Vulnerability-Asset Worksheet, Risk Assessment

Jaden Howell- Additional Measures, Access Control Policies and Implementation, Intrusion Detection System Policies and Implementation, Firewall Policies and Implementation

Table of Contents

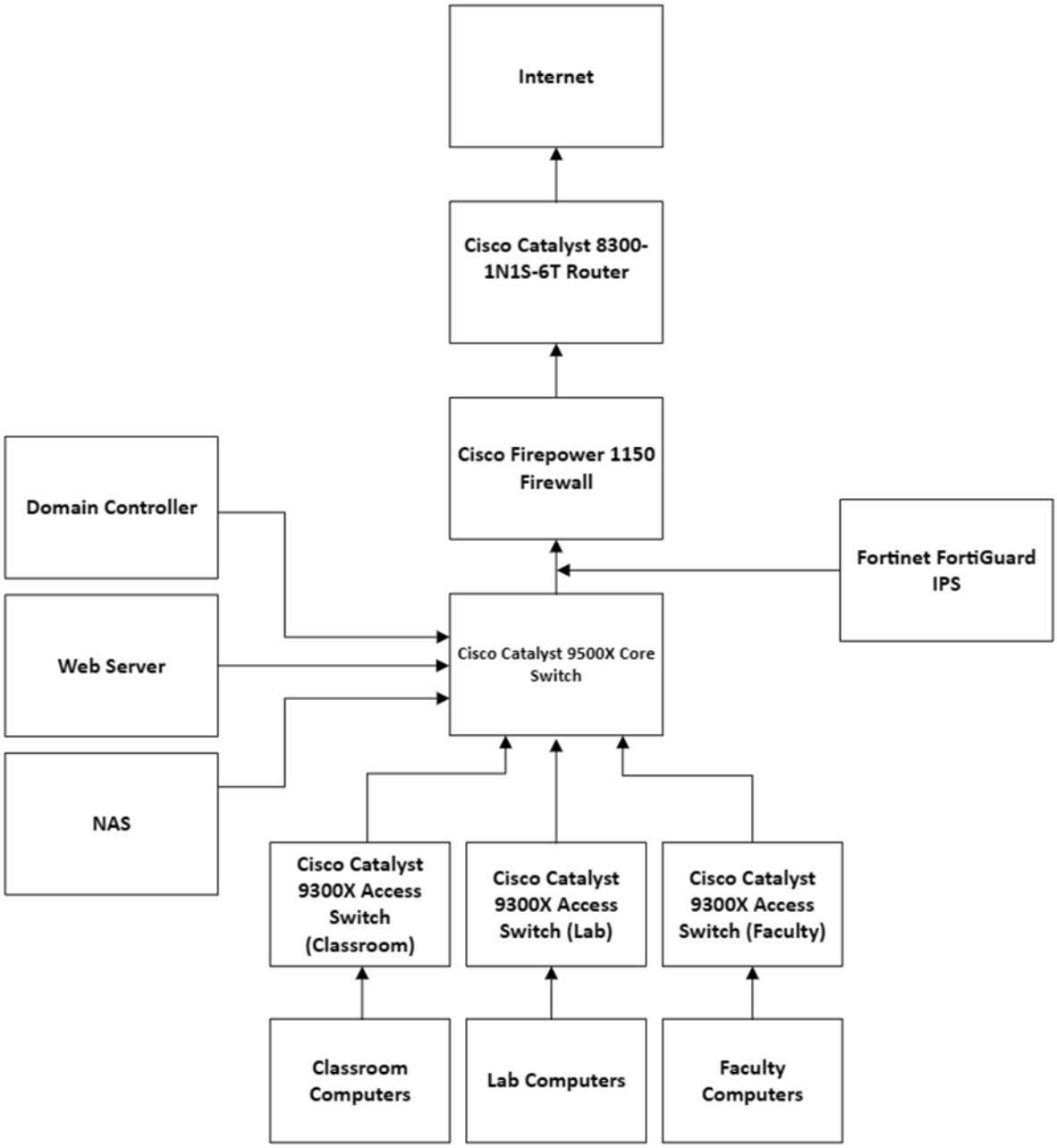
Introduction

During this report we will discuss our approach to designing a secure network for the Strome College of Business (SCB). The SCB domain name is SCB.odu.edu. The SCB is made up of three wired subnets which include labs, classrooms, and faculty offices each with no more than 200 computers per subnet. Microsoft Windows and Cisco products will make up most of our network infrastructure. A network diagram will be provided with further explanation as to our design and decision-making process. Potential threats and attacks will be an area of focus as cybersecurity has never been more important. We will conduct risk analysis and list our policies to mitigate risk as much as possible. Confidentiality and authenticity will be covered through the use of encryption and VPNs. Access control policies, firewall policies, intrusion detection systems policies (IDPS) will all be covered. Host hardening, our approach to security for software and applications, data protection measures, incident response plans, and disaster recovery plans will also be discussed. Risk will be reassessed with these updated controls.

Mission Statement

Our mission is to design a secure, reliable, and scalable network for the Strome College of Business. Security is a key point for our design as we aim to protect the faculty and students from those with malicious intent. We aim to ensure that the network is as reliable as possible so that faculty and students do not experience interruptions. Scalability is essential in the case that the business building expands. By designing our network with scalability in mind we ensure that the SCB is not limited by network infrastructure.

Network Diagram



Network Diagram Explanation

When designing our network, we made sure to focus on choosing hardware that would ensure security and reliability, while also allowing for scalability down the road. Choosing products that were a good fit while not wasting money was another key factor in our process. These factors made the Cisco Catalyst 8300 1N1S-6T router an ideal choice for the SCB network. The 8300 features SD-WAN IPsec throughput of up to 2Gbps, IPv4 forwarding throughput of up to 19.7 Gbps, 4,000 IPsec SVTI Tunnels and ACLs per system, 72,000 IPv4 ACEs per system, 1.6 million IPv4 Routes, 1.5 million IPv6 routes, 8,000 queues, 1.2 million NAT sessions, 512,000 firewall sessions, and 4,000 VRFs. These performance metrics make the 8300 more than enough for the SCB.

We chose the Cisco Firepower 1150 firewall for its first-rate security specifications and features. The 1150 provides firewall throughput of 4.9 Gbps, IPS throughput of 6.1 Gbps, IPSec VPN throughput of 2.4 Gbps, and up to 800 supported VPN peers. These specifications make the 1150 a great fit for the SCB while also abiding to the requirement of using Cisco products. The Fortinet FortiGuard IPS Service was chosen to detect and prevent security breaches from reaching the SCB network. The Cisco Catalyst 9500x core switch and 9300x switches were chosen for their reliability and features which allow for scalability. Our design ensures security and scalability of the network while not wasting money unnecessarily.

Possible Threats and Attacks

- **Espionage and Trespass**
  Unauthorized access to systems poses a major risk to the SCB. If a hacker were to gain access to ODU systems, they could access personal and financial information of students and faculty. Through proper information security measures such as firewalls, intrusion prevention systems, and information security policies and training we can lower risk.

- **Lack of Authentication and Regular Password Changes**
  Login portals which don't require two factor authentication and frequent password changes put a network at risk. For this reason, we will require two factor authentication through Cisco's Duo. Frequent password changes will be required, and online training will be provided for proper password policy.

- **Forces of Nature**
  With the building being elevated, flooding isn't much of an issue, however, a fire breaking out could compromise information security. If left untamed a fire could destroy critical network infrastructure. To mitigate this risk, we will make sure that fire extinguishers are located throughout the building.
- **Human Error**
  Students or faculty could compromise network security through mistakes or by ignoring policies. For example, if a faculty member shared their ODU account

information with others. This could lead to security threats if the information were to fall into the wrong hands.

- **Phishing**
  Email phishing attacks are one of the most prevalent threats to network security. Phishing attacks work due to the senders posing as a trusted person or company who is requesting personal information. By informing students and faculty of these attacks through frequent training the effectiveness of phishing attacks can be lowered.

- **Extortion**
  If an information technology faculty member were black mailed network security could be at risk. Though unlikely a faculty member could be forced to give up sensitive data or information.

- **Technological Obsolescence**
  Outdated technology or practices could put the SCB network at risk. For example, computers with outdated operating system versions will lack the security patches that updated systems will have. To ensure network security we must do routine maintenance including installation of new updates.

- **Malware and Ransomware**
  Malware and ransomware can gain unauthorized access to systems, often causing damage. To protect our network, we will install Windows Defender antivirus on all supported devices.

- **Physical Security**
  In the event of an individual or group attempting to physically attack or dismantle our networking equipment, security or the police will be contacted. Monitored security cameras will also be located throughout the building.

Planning, Organization, Risk Analysis, and Policies

To ensure network security, we will take a preventative approach which focuses on planning. The Chief Information Security Office will head the IT department and will manage the other staff in the IT department. There will always be some level of risk involved with operating a network, however, we aim to mitigate risk as much as possible. The threats and attacks discussed earlier are some of the major risks which our network faces. We will conduct a risk assessment to better identify and categorize each risk factor. Threats will be identified, vulnerabilities will be listed, and impact and risk will be assessed. Access control policies and firewall policies will be implemented and will be discussed later in this report. The IT department will be responsible for implementing and ensuring compliance with policies.

Threat-Vulnerability-Asset Worksheet

Asset	Threat	Vulnerability	Impact	Risk	Mitigation Strategy
Data	Ransomware, malware	Human error, lack of encryption or poor encryption	Data breach	High	Encrypt data, frequent training
Network	DDoS attacks, malware, zero-day exploits, phishing	Misconfigured firewall, lack of access controls, outdated software, human error	Security breach, network downtime	High	Proper firewall configuration, access controls, update software, frequent training
Hardware	Failure of hardware or theft	Old hardware, incompatible hardware	Security breach, network downtime	Medium	Replace hardware when necessary, make sure hardware is compatible
Software	Malware	Lack of or failure of antivirus, human error	Security breach	Medium	Make sure antivirus is installed and updated
People	Phishing, theft, extortion	Human error	Security breach, network downtime	Medium	Frequent training
Firewall	Malware infiltration, network breach	Misconfigured firewall	Security breach, network downtime	High	Proper configuration of firewall

Risk Assessment

The threat-vulnerability-asset worksheet displays the threats and vulnerabilities involved with each asset in our network as well as the impact of each threat and the mitigation strategy to handle risk. By analyzing the risk of each asset, we have come to the conclusions shown in the mitigation strategy column. The cost of additional training and security measures is greatly outweighed by the increased security of our network. Loss of sensitive data or downtime of the network could result in the loss of thousands of dollars. By applying these strategies, we will be able to mitigate risk substantially, ensuring a secure network.

Additional measures for the best confidentiality

The network will feature a standardized sign-in and sign-out process. Each individual will be assigned a username and will create their own password, which will only be stored by us for data recovery purposes. To verify identity, users will be required to download the Duo Mobile app or use a physical issued Duo-100 device so we can monitor when they try to sign in. Whenever a user seeks to access any system within Constant Hall, they must confirm their identity through Duo. Additionally, confidentiality will be maintained through encrypted data, with strict access controls to prevent unauthorized users. We will implement AES 256-bit encryption. Additional security measures will include:

- Implementing policies to further strength effectiveness, such as network access control policies
- Prohibiting any external devices such as USB drives to be plugged in without verification for personnel first
- Including data backups at the end of the night or at least in a 24-hour cycle to ensure the safety of sensitive data.
- Sending out regular updates and patch notes on hardware and software systems throughout the course of the year
- Having antivirus security installed on all systems
- Having strong physical access to the main rooms in the building such as server rooms, data rooms, and other main points of the network infrastructure.
- Allowing pen-testers to try and find any vulnerabilities in our systems so we can improve them for the future.
- Having honeypots within the system to better secure the real systems.
- Managing mobile devices access in the organization's network with MDM solutions
- Before including any third-party organizations, check their levels of security and infrastructure.
- Using VPNs whenever accessing sensitive data from a remote place that is not the main infrastructure.

Having these additional security measures will likely increase the protection of all the systems within the infrastructure and we will continue to add more as the systems continue to grow and evolve with the organization.

Access Control Policies and Implementation

The individual will be responsible for ensuring that access controls are properly implemented in alignment with the security policies, standards, and procedures set by Old Dominion University. This includes ensuring compliance with all bodies of law and regulations regarding access to university systems and data. The role requires a deepened understanding of the university's security framework and the legal requirements that govern the protection of information. Access controls must be established and maintained to ensure that only authorized users have access to sensitive information and systems, preventing unauthorized access and protecting against potential security breaches. The individual will also need to monitor and review access control systems regularly to ensure they are functioning effectively and remain compliant with both university policies and external legal requirements.

Management of Accounts: Accounts will be created for any user authorized by the organization, allowing them to access various systems and services on campus. Usernames will be unique to each person utilizing their names and numbers as well as a special character.

Management of Passwords: To keep maintaining secure and strong passwords, there are strict password requirements to ensure that they will not be easily guessed or cracked. The minimum requirement for the password is that it has 15 characters including an upper case and a lower-case letter, one number and one symbol to meet the minimum requirement. At first when given an account, you will be given a temporary password that you will use to log in and then set up your own password from there.

Mobile Devices Access Control: Unless authorized by one of the supervisors or anyone with the credentials, mobile devices should not be connected to the network to reduce traffic.

Wireless access: All authorized users will be allowed to connect to the wireless network. When they try to connect, they will have to provide a username and password to be able to sign into the desired wireless network.

Remote access: Authorized users are allowed to access the network through a secure VPN. Connecting to the VPN will be through the same username and password.

Permitted Actions without Authentication: Any system that is connected to the network will need the proper identification in order to access it.

Unsuccessful Login attempts: All users have 4 attempts to log in with their correct username and password into the system. After that last attempt, their account will be locked for 15 minutes. If it happens again then it will be locked for 30 minutes. After that they will need to contact the IT help desk to verify and reset their password.

Notifications of System Use: All users must agree to the system use policy before having access to any of the systems. That way they are held accountable for all their actions that they do regarding the Universities systems.

Summary

This section outlines the compliance requirements for the Access Control Policy. Following these guidelines is necessary to ensure proper management and monitoring of access to sensitive information and systems. Compliance helps meet legal, regulatory, and ethical standards, ensuring that only authorized individuals can access important data. By following the Access Control Policy, the organization reduces the risk of unauthorized access, data breaches, and other security issues. The policy limits access based on the principle of least privilege, giving individuals only the permissions they need for their roles. This strengthens security and ensures compliance with laws and regulations that require strict controls over sensitive information. The policy also includes regular monitoring and auditing of access to detect potential security issues. Periodic reviews of access controls are required to ensure they remain effective and adapt to new threats and changes in regulations. Complying with these guidelines is essential for maintaining a secure and legally compliant environment for all users and systems. Once they sign the user agreement, they will have authorization to utilize the various systems in the infrastructure and are responsible for their own account and actions.

Firewall Policies and Implementation

Creating strong firewall policies for the Strome College of Business network is essential for protecting its infrastructure from unauthorized access, cyberattacks, and other security risks. A solid firewall strategy includes setting clear policies, choosing the right firewall technologies, and configuring rules that fit the college's network needs. The process involves defining what traffic is allowed or blocked, ensuring the firewall is properly set up, and regularly reviewing its effectiveness. This approach helps secure the network, prevent malicious activities, and maintain safe communication between systems. Below are suggestions of some ways to implement these firewall policies:

- Allow only the necessary protocols and services when implementing firewall policies
- Defining rules for the flow of traffic to protect it from external threats
- Implement break downs with segmentation to control traffic between different internal segments
- Using the proper communication between internal resources while limiting unnecessary use of traffic
- Establish secure VPN policies for remote access
- Ensure the encryption of data
- Making sure to constantly review and revise firewall policies to adapt and evolve along with the network and security
- Conducting regular assessments with security to properly identify and address threats that could potentially emerge from the systems
- Enabling logging for the activities for firewalls
- Making sure to regularly review logs to be on the lookout for suspicious activates
- Introducing mechanics to alert the users that there may be potential security incidents

- Making sure to educate users about the importance of firewall policies and making sure they understand the importance of practicing good security measures
- Making sure to educate the importance of reporting any suspicious activities to prevent further threat
- Clearly defining roles and responsibilities to user in the event of a security breach
- Having an incident response plan that has the procedures for handling all incidents related to firewalls
- Having audits regularly to ensure that the policies are kept up with
- Installing firewall configurations that align with the industry's best practices to ensure better security protection.

Intrusion detection systems policies and implementation

The purpose of our Intrusion Detection/Prevention System is to identify potential security incidents, both large and small, by monitoring the network and logging any suspicious activity. Any alerts generated will be taken seriously, thoroughly investigated, and reported to our security administrators. The IDS/IPS will play a key role in helping the Strome College of Business protect sensitive and confidential information by detecting attempts to bypass security measures. The IDS/IPS will continuously monitor the network for unusual activity, enabling the detection of any potential breaches or new threats. This proactive approach minimizes the risk of significant damage by catching problems at an early stage. The system will provide real-time data on anomalies in several critical areas, helping ensure that the network remains secure and resilient against evolving threats. This approach is crucial for maintaining the integrity of the network and protecting valuable information from unauthorized access. The tools that will be used will show activities in these areas:

- Internet traffic
- Mail traffic
- LAN/WAN Traffic
- LAN/WAN Security Protocols/Analysis
- Operating System security
- Malware detection
- DDos/DoS Protection
- Vulnerability Detection
- Anomaly detection
- Content Inspection
- Signature Based Detection

In addition to the different areas that will be constantly monitored, the files will have to be checked for vulnerabilities or if they are at risk of exploitation. The primary files and log access that will be checked are:

- User accounts

- Network
- Web servers
- Database
- Domain
- Firewall
- System error
- VPN
- Physical Access
- Data backup/Recovery
- Endpoint security
- Authentication/Authorization
- Automated Intrusion detection systems

The minute that the intrusion detection system detects any issue, it will be sent to the security administrators, and they will work immediately to fix the issue. Reports will be made of any major intrusion that causes setback and/or damage.If an attack is detected, IT and security personnel will immediately check the system for updates. An investigation will follow to determine if there has been any breach or data leak. Authorized administrators will look for any anomalies, patterns, or unusual behaviors that could indicate a security incident. They will also correlate information from the Intrusion Detection/Prevention System with data from other security tools and logs to understand the full scope of the incident. If a system is found to be compromised, it will be shut down and isolated from the network to prevent further damage. In the case of a breach, the threat will be identified and removed from the system. Additionally, any vulnerabilities will be patched and updated to prevent future attacks. This process helps ensure that the network remains secure and any potential threats are addressed promptly.

Host Hardening with Update Policies and Implementation

Host hardening methodology is the steps taken to ensure that a system is secure by a simpler but more strength-focused approach. This critical process includes actions that involve removing components of a physical/security system that are susceptible to attacks while not being totally necessary to a security system by having alternatives that harness less of a vulnerability and provide a stronger force of security. Removing a system's attack surface to the point where there are less areas of possible attack targets play a significant role in keeping a system of network security strengthened. Host hardening measures can be applied universally to any system, such as Strome College of Business' many servers and network devices through tactics. These host hardening tactics such as update policies and implementation can be done with several methods:

Host Hardening:

Device and Network Authentication:

- Implement the concept of using strong passwords and/or pins.

- Authentication methods such as two-factor authentication or multi-factor authentication.
- Utilize biometric authentication methods such as facial scanning and fingerprint matching.
- Personal security questionnaires if troubles with password entering occur.
- Ensuring that each of the 200 computers are secured with password entries upon access.

Data Encryption:

- Utilize high standard encryption landscapes, such as symmetric encryption with the AES (Advanced Encryption Standard).
- Encryption must be accurately implemented into servers and networks.
- Authenticate proper access roles to encryption data and information.

Proper Awareness and Training Methods:

- Ensuring that adaptable routine education panels are performed to keep employees up-to-date on current policy information and operational details.
- Enforce cyber-hygienic training procedures to mitigate the chances of phishing scams and accidental malware downloads.
- Emphasize the importance of updating user devices.

Firewall Implementation Security Measures:

- Access-control devices used to approve/deny specific traffic from network entry.
- Pre-implementation testing methods on firewall devices such as the Cisco Firepower 1150 to ensure capabilities before touching actual systems.
- Ensure firewalls are placed in useful and correct areas of needed security to ensure redundancy and no chance of failure.

Removing Unnecessary Components:

- Revoking certain device operations to lessen the chance of an attack.
- Limit the capabilities to role-based access to ensure authentication in certain areas of the system.

Creating an Incident Response Plan:

- Curating an adaptable, consistently updated incident response plan that can be adhered to many forms of incident categories.
- Routinely carry out these response plans regardless if an incident occurs.
- Utilize predictive knowledge to become the backhand of preventing incidences.

Host Monitoring:

- Utilizing detection and monitoring systems for identifying undesirable patterns of data flow that could act as a threat to the security systems.

Least Privilege:

- Grant low level access permissions to certain networks and roles among the 200 computers and several network devices to ensure proper availability and authentication.
- Harden the system by removing unnecessary privileges from users who do not need to be granted access.

Update Policies:

Security Updates:

- Regularly downloading and updating systems as scheduled to patch/prevent any system vulnerabilities from occurring.
- Enabling updates to install automatically for less issues manually implementing updates.
- Ensuring anti-virus updates are installed into systems both physical and digital.
- Enforcing regular audits to make sure updates are contributing to success.

Updating Operating Systems:

- Scheduling regularly operating system maintenance to ensure that there is no room for error or known vulnerabilities.
- Security Updates stated above should be thoroughly implemented into the software system update.
- Disabling components of the operating system that would act as a greater attack surface for an intruder.

Strome College of Business having these proper host hardening policies with consistent implementation routines can grant the ability for security systems to be adequate. These policies and methodology provided above acts as an adaptable framework for the best practices of hardening a host system. Through update policies, operating system updates, physical system planning, and enforcing routine security measures can ensure a small attack-surface within the Strome College of Business' system.

Application and Software Security Policies

Software security policies are among the key components to keeping the Strome College of Business safe and secure digitally. Old Dominion University harnesses a strong layout for technology policies in order to keep users safe who use the provided resources, including the many servers and networks located inside Strome College of Business. Software policies in this case should reflect on what measures are needed in order to provide a strong physical system structure while also having reinforcements digitally to safeguard software systems from vulnerabilities and flaws. There are multiple software and application policies that should be used when discussing the best protection methods for software and

application systems:

Software Policies:

Acceptable Use:

Users must utilize the provided resources for intended purposes only such as educational related purposes for specific access-level users. Employees must use devices for organizational purposes and refrain from utilizing resources for personal or malicious acts that do not align with assigned roles.

Data Handling:

Data can only be used and processed by authenticated individuals or through applications that are authorized for granted use of data processing. Compliance measures must be met in order to prevent vulnerabilities and threats from occurring due to mishandling of data. This includes all users who access resources within the premises and cover personal and institutional data.

Necessary Updates:

Regulatory updates are mandated in order to ensure proper measures are up to date. Security updates such as anti-virus, malware, monitoring, and intrusion system updates are mandated to ensure there is no room for error. Software and application updates are mandated regularly as well to ensure that systems are current with the proper security measures and components in place.

Awareness and Education Training:

Routine awareness and educational training for employees ensure that individuals gain the adequate amount of resources and knowledge about operational aspects of software and security systems within the Strome College of Business. These routine educational training audits can be used as demonstration follow-ups for data handling, security update implementations, and digital hygienic practices to ensure users are well educated on how to properly handle data. Routine procedures are crucial in keeping users current with system changes and new implementations in policies.

Incident Response:

This policy considers measures that are desired for handling valuable data if an incident were to occur. There is a focus on recovery plans, mitigation attempts, and legal compliance with a proper incident response policy. Incident response plans cover a variety of cyberattacks and showcase proper response methodology for when one occurs. These attacks can be identified as: malware implementation to dismantle networks or malicious attacks for the purpose of data theft.

Logging and Monitoring for Applications

This ensures that behavior within a network, software, or application is monitored and logged into a database so therefore can be revised for anomalies that can pose as vulnerabilities. Logging methods keep history of any attempt to gain access to information

within the network.

Data Encryption Policy

Data within a software system can only be encrypted by authorized individuals who are granted technical access into the system. Data must be encrypted through high-standard algorithms such as symmetric and asymmetric encryption, and used with standards such as AES or RSA.

Authentication Policies

Only individuals who have authorized access into the system can be granted permission. This includes employees who are in higher roles such as information security management officers and builders. Users who operate on a server that is granted least privilege cannot be granted access into security logs and operational settings. Devices such as two-factor authentication, multi-factor authentication, and biometric authentication devices will be mandated to ensure proper individuals are granted access.

Access Control Policies

This policy applies to all individuals who participate in the use of digital devices within the network of Strome College of Business. This determines the access of data and information and who has the permission to operate on these levels. This policy utilizes least privilege methodology, authentication methods, auditing to ensure the granted individual has access based on certain criteria.

Data Protection Measures

Data Protection Policies

Data protection policies are implemented for the purpose of protecting sensitive information in regards to individual, business, and employee information. Data protection policies within Old Dominion University's borders revolve around the networks, computers, internet, databases, printing, and telecommunication equipment for how they are utilized. Many data protection policies include expected responsibilities for when an incident occurs within a system. These responsibilities include complying with and analyzing university technology requirements, reporting of incidents or suspected incidents to the university management or information security officer. Visitors are also responsible under the guidelines, such as vendors, family of students, volunteers, guests, uninvited guests, and all persons on property, owned, and leased by the University. Some of Old Dominion University's include, but are not narrowed to:

Data Administration Policy:

Purpose

The purpose of this policy is to regulate the administration of University's data. This is subsidized by an established framework that shows a need for a policy creation.

Scope
This policy is made for all individuals who utilize Old Dominion University's technological resources. This includes all employees, students, volunteers, and visitors. This policy involves all data that is provided, used, or maintained by Old Dominion University regardless if it is shared or networked. This applies to all information that is found on equipment that is owned by the university.

Policy Statement
From the official Old Dominion University website, "Data classifications and associated protective controls account for academic and business needs for sharing or restricting information and the impact associated with such needs. Data classification informs security decisions such as location of stored data, authorization and access requirements, continuity of operations and disaster recovery planning, and are maintained in risk assessment documents."

With this data protection policy in place at Old Dominion University, there is understanding that this policy also covers the Strome College of Business as it harnesses digital property that is provided by the University.

Data Protection Technology

There are quite a few ways that organizations such as the Strome College of Business can go about protecting data through devices and software. There are a few subjects to consider:

- Access control methods such as two-factor authentication, multi-factor authentication, and biometric devices that are used for data protection.
- Anti-virus application implementations that can be used to protect systems from obtaining a virus or malicious code.
- Physical security measures such as keeping systems in isolated locations safeguarded by passkey or biometric entry.
- Regular routine auditing to overlook data systems for any vulnerabilities present that can be known to put data and information at risk.

Backup Storage Locations and Recovery Measures

Considering the layout of Strome College of Business, there is an understanding of how space can be utilized for storage locations. The two-floor building has the ability to house closets on each floor which can be used as storage rooms for redundancy. These rooms are where backup systems and physical data devices can be stored in case of an emergency. This method of backup storage can go hand-in-hand with an incident response plan to ensure that the Strome College of Business ensures a successful recovery with backup storage. Recovery measures can include allowing for redundancy between the networks by having more than one connectivity device with different setup specifications to ensure

proper authentication. If one system is breached then it would not call for a total shut down between all systems.

Specifications

- https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8300-series-edge-platforms/datasheet-c78-744088.html
- https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/intrusion-prevention
- https://www.cisco.com/c/en/us/products/security/duo/what-is-duo.html
- https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html
- https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
- https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html
- https://www.microsoft.com/en-us/windows/comprehensive-security?r=1

Bibliography

One Identity: One Identity. (n.d.). *What is strong authentication in cybersecurity?* One Identity. https://www.oneidentity.com/what-is-strong-authentication-in-cybersecurity/#:~:text=The%20universal%20way%20to%20strengthen,to%20do%20their%20job%20tasks

TrustCloud: TrustCloud. (n.d.). *Host hardening documentation: A comprehensive guide*. TrustCloud. https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/host-hardening-documentation-a-comprehensive-guide/#:~:text=Host%20hardening%20refers%20to%20the%20process%20of%20securing%20a%20computer,firewalls%2C%20and%20implementing%20access%20controls

Engage for Success: Engage for Success. (2021, May 11). *7 cybersecurity awareness best practices for employees*. Engage for Success. https://engageforsuccess.org/crisis-and-change/7-cybersecurity-awareness-best-practices-for-employees/#:~:text=integrate%20security%20training%20into%20the%20onboarding%20process.,teaching%20employees%20how%20to%20identify%20and%20prevent

Microsoft: Microsoft. (n.d.). *Software restriction policies*. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies

Micro Focus: Micro Focus. (n.d.). *About software policies*. Micro Focus. https://docs.microfocus.com/SA/10.51/Content/SwProv_UG/software_management/AboutSoftwarePolicies.htm

Whitman & Mattord: Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage.

Satori: Satori. (2023, April 22). *Access control policies: Definitions & types*. Satori Cyber. https://satoricyber.com/access-control/access-control-policies-definitions-types/

BasuMallick: BasuMallick, C. (2022, March 4). *Top 10 intrusion detection and prevention system software in 2022*. Spiceworks. https://www.spiceworks.com/it-security/vulnerabilitymanagement/articles/best-idps-software/