Management of Information Security Project Report
Network Infrastructure Design

Connor G., Seth D
IT417: Management of Information Security
Dr. Kalburgi
December 2, 2024

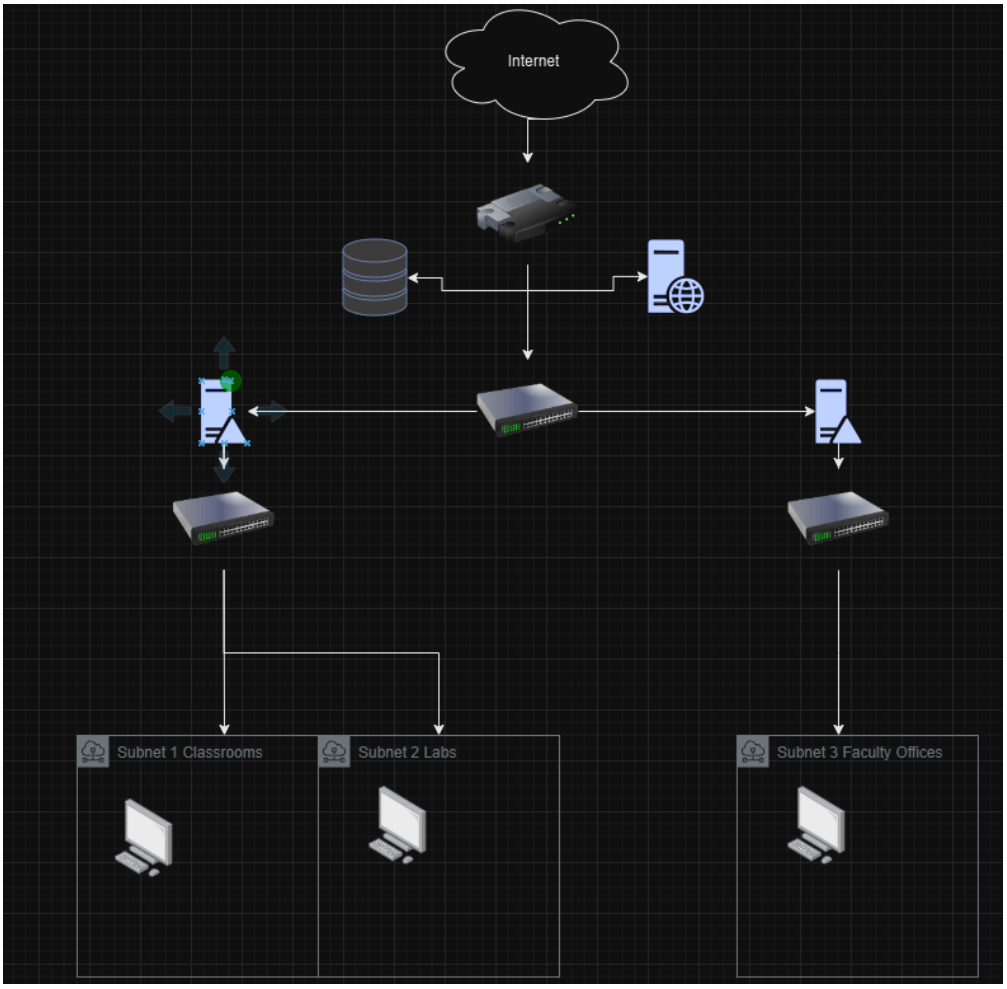
Table of Contents

Introduction of the Problem

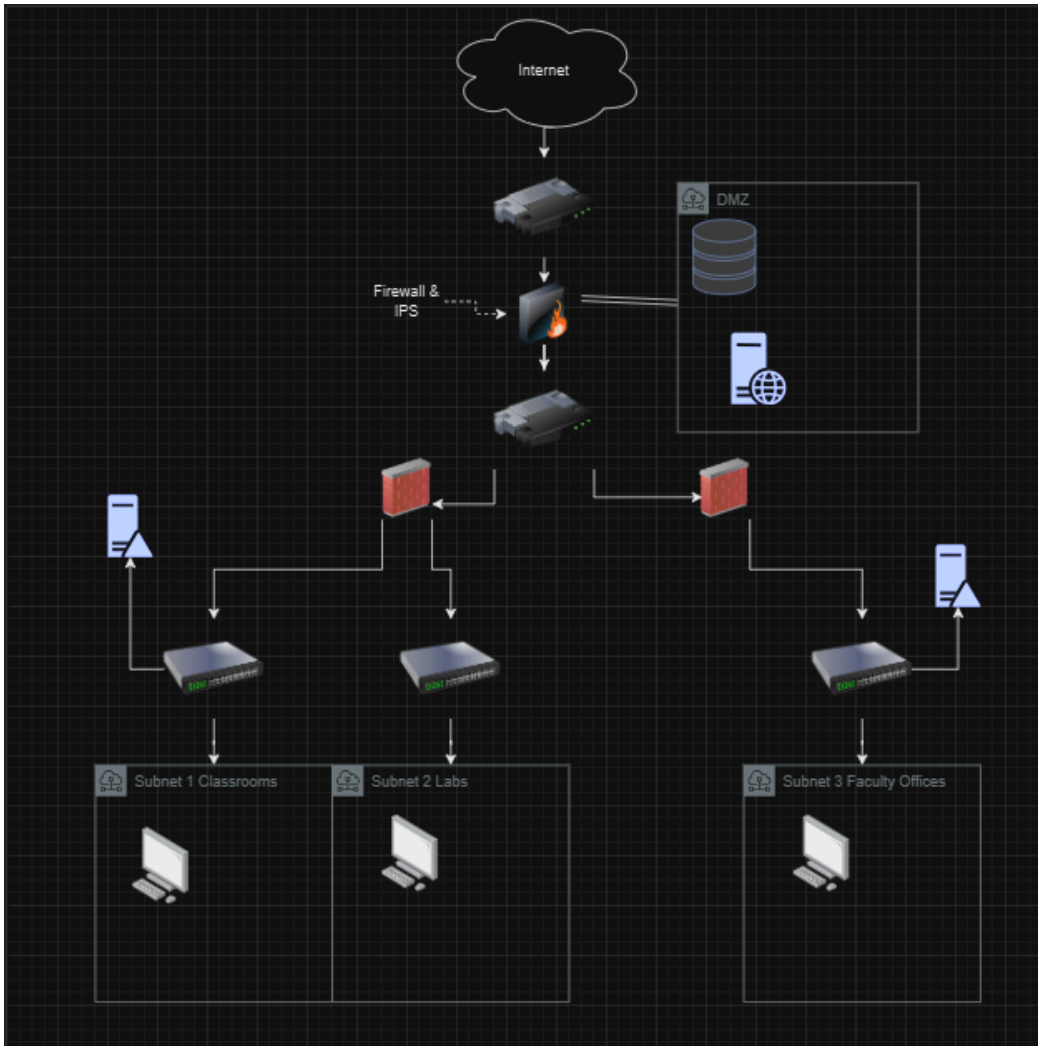
Strome College of Business has a network (SCB.odu.edu) spread across multiple floors, labs, classrooms, and faculty offices. Currently, there is little security across these systems. This is a massive problem due to the amount of sensitive data, secure records, devices, and other major systems that could be affected if there was an attack or breach. Not only could these systems be broken into, but attackers could potentially interrupt classroom activities inside Strome. It is clear that changes need to be made, both to the organizational side as well as the physical systems within Strome.

"Our mission is to create a secure network within Strome College of Business to safeguard the Confidentiality, Integrity, and Availability of information systems and to ensure the continued security of the organization through proper security policies, updates, and monitoring".

As seen below in the first diagram, The original network is situated with a router facing the edge, connected to it is our web server, NAS, and a switch that leads down to our two domain controllers, which both connect down into the three subnets. One connects to two of our subnets; Classrooms and Labs. The other one connects to the subnet for Faculty offices. Each of these subnets has around 200 computers in each. This network is utilized daily and is frequently used by both students and faculty, accessing the internet and other services and files stored in the university NAS.



From the original diagram, it is easy to see that physical upgrades and changes in various areas are needed. The network consists of many different vital areas for the continued use of the network by students, but it also consists of the critical sensitive data that a university may be using at any given time. With this design, this sensitive information is not secure enough and needs to be protected by the network.



Our re-designed network operates around a Screened-subnet DMZ firewall, with logical firewalls as secondary filters separating the subnets. The DMZ is used to house the servers so that the untrusted traffic is directed directly to the servers instead of coming through the network. The domain controllers are located in central locations in which they are most accessible to the users.

Possible threats and attacks

As seen in the original network diagram, there is relatively little protection for our original network. In order to bring our network into compliance with our mission statement, we must conduct a Threat Assessment of our network and use the information to strengthen the vital areas of our network. Our university network is extremely vulnerable to several threats, both internal and external. For example, little security systems in place leave our network vulnerable

to Espionage/trespass, theft, extortion, and attacks on both students and the University. The local web server for the Strome building is left relatively undefended, leaving countless possibilities for defamation of web pages, information theft, or other software attacks. Little or no role provisioning may allow student computers from within the organization to access files or data not meant to be accessed by the students. Out of the twelve categories of threats to Information security, we Identified six threats that could impact our current network outside of the usual threats faced by all networks such as quality of service deviations or forces of nature. The first threat category we identified was “Compromises to intellectual property”. This threat involves software piracy or other copyright infringement activities. Our network currently has little to no security controls, potentially allowing an attacker to compromise University intellectual property. The next important threat category we identified was the “Espionage or trespass” category. In this setup, our network could easily be trespassed into for unauthorized data collection or access to the systems. Due to this any information across our network from IDs and passwords to students gaining access to secure portions of the network they are not supposed to access. The next threat category is “Information Extortion” across the network. Many different students and faculty members are accessing this network, and without our security recommendations in place, there is a threat of information disclosure from the personal data used by the university. The next threat category faced is “Sabotage or vandalism”. Our network is open for users to be able to knowingly or unknowingly destroy systems and information, this is an area where we must use roles and other security policies to mitigate any issues on this threat. “Software attacks” such as malware, denial of service, or other forms of attack are another large threat area for our network. Without a dedicated monitoring system in place, our network and its users could be at risk of software attacks. This category also describes various attacks our network may face. The last major threat category that our current network is vulnerable to is “Theft”. This category aligns with some of the other threat categories, this network could allow a third party to illegally confiscate information from our network, another threat area we will seek to mitigate. The other threat categories such as “Forces of nature” will equally affect all information systems, this threat will be mitigated by our disaster recovery plan. Technical hardware or software failures are always possible, along with technological obsolescence. Each of these is a significantly smaller threat when compared to the current vulnerabilities present in the network.

Planning, Organization, Risk Analysis, and Policies

Given that we have now recognized the threats which our network may face. We may now plan our next steps for security in our network. In order to set clear goals and objectives we must clearly analyze how our current network is affected by the identified threats. In order to assess the network and its vulnerabilities so we can analyze the risk, We created this Threat Vulnerability asset worksheet of the original network so we can assess what in the original network needs to be improved upon.

	Asset 1 Web Server	Asset 2 NAS	Asset 3 Routers	Asset 4 Domain Controllers	Asset 5 Computers
Threat 1 Software Attacks	T1V1A1 T1V2A1 T1V3A1	T1V1A2 T1V2A2 T1V3A2	T1V1A3 T1V2A3	T1V1A4 T1V2A4	T1V1A5
Threat 2 Espionage/ Trespass	T2V1A1 T2V2A1 T2V3A2	T2V1A2 T2V2A2 T2V3A3	T2V1A3 T2V2A4	T2V1A4 T2V2A5	T2V1A6
Comprimises to intellectual property	T3V1A1 T3V2A1 T3V3A3	T3V1A2 T3V2A2 T3V3A4	T3V1A3 T3V2A5	T3V1A3	T3V1A4
Threat 4 Information extorsion	T4V1A1 T4V2A1	T4V1A2 T4V2A2	T4V1A3	T4V1A4	T4V1A5
Threat 5 Sabotage/ Vandalism	T5V1A1	T5V1A2	T5V1A3	T5V1A4	T5V1A5
Threat 6 Theft	T6V1A1	T6V1A2	T6V1A3	T6V1A4	T6V1A5
Threat 7 Technical Hardware Failure	T7V1A1	T7V1A2	T7V1A3	T7V1A4	T7V1A5
Threat 8 Human error	T8V1A1	T8V1A2	T8V1A3	T8V1A4	T8V1A5
Threat 9 Quality of service deviations	T9V1A1	T9V1A2	T9V1A3	T9V1A4	T9V1A5
Threat 10 Forces of Nature	T10V1A1	T10V1A2	T10V1A3	T10V1A4	T10V1A5
Threat 11 Technical Software Failures	T11V1A1	T11V1A2	T11V1A3	T11V1A4	T11V1A5
Threat 12 Technological obsolescence	T12V1A1	T12V1A2	T12V1A3	T12V1A4	T12V1A5

With this view of our systems and their threat vulnerabilities, we are able to create a plan to decide what modifications to make to our network, as well as our organization and the policies that we will be utilizing. Proper planning for our organization and how we plan to upgrade our systems and policies comes first. With this assessment complete we can create security goals for our organization. Our main goal is to provide immediate protection of the sensitive information on both the network in our web server and the various systems across the network. Our next goal is to create policies and organizational efforts to manage the network so the network will never fall into a similar unprotected situation again. As an organization, we must make an effort to plan our actions ahead of time. This will include planning the updates necessary to secure the network as it currently stands but also to plan for the future of the systems. As well as planning activities, there are Organizational changes we can make to improve security. An example such as the appointment of a security team is a necessary start. If not already in place, a security team of Network Administrators, IT specialists, and management members. This team will be

responsible for the security of the network, as well as maintenance and threat monitoring to keep the network working and safe.

Strict basic policy changes are also needed. In order to protect Strome's information assets, we must create a strong organizational security policy that focuses on the need for security. The policies will need to apply to all members who utilize the business school for them to be effective. This is a large task that will set the standards for which all of the devices on the network will need to be compliant. It involves creating policies relating to access control, firewall management, IDPS management, host hardening, software security, data protection, and incident and disaster recovery.

Measures taken to provide information security

Measures taken to ensure confidentiality

An important function of a network is to make sure that all of the data flowing through the network is safe, secure, and confidential. One way to make sure that data in transit is secure is by using secure protocols, like HTTP, S/MIME, SSH, WPA2, and many others. All of these protocols were designed to make sure your data is more secure in comparison to their unsecured counterparts. Another way we will ensure confidentiality is to make sure that user data is only accessible to that user and authorized user. This can be done through the implementation of access controls, which will be talked about more in-depth in the next section. But, this is one way we will ensure confidentiality.

The use of VPNs will be part of our plan to provide secure and confidential access to files and the network. The use of VPNs is typically are cases when a user wants to connect to our network from an outside source. We use the VPN for this purpose because it has the ability to create a secure connection to our network even though it goes through the internet instead of a direct connection. The VPN protocols themselves are already secure but we need to ensure that the person connecting to the VPN is who they say they are. For our network, this feature does not need to be available to everyone. The users who would be authorized to use this would be users who were granted special access to this service.

Access control policies

Access control is essential for assuring access, integrity, confidentiality, and maintaining a secure network. It is the system in which users are granted access to various parts of the network and systems necessary for their job, task, or project. This system is responsible for deciding if users who request access to a resource are authorized to access that resource.

To create access controls we need to cover the four fundamental functions. The first is identification, which is making sure that a person trying to access the system is a valid user. Second, is Authentication, which builds off the first step because it is where the person proves they are the user identified. The person needs to prove it with something they know, something they have, and something they are. Next, is Authorization, which is where the system matches the authenticated user with the corresponding access level. Lastly, is Accountability, which is when the system keeps track of what each user does on the system.

The original network has very little of these systems in place. In the original network design, it has no way of controlling access, so everyone can access everything. This is a problem because then everyone can access important documents and information. This leads to information leaks and the data within these documents have the risk that files could be changed without the owner's knowledge. Anyone will have access to the network from any computer on any subnet. It also has no way to authenticate if the user is who they say they are, which could lead to completely random people stealing a student or faculty username and password to get access to the information on the network.

In order to comply with our mission statement we need to implement access controls to the network. There are many different ways of implementing access control, the one we have chosen for our network is role-based access control. This decision was chosen based on the needs of the network. Role-based access control allows for controls to be assigned based on what roles a user needs to fulfill. For our network, we would need many roles, Student, Faculty, Staff, and Administrators. Those roles are basic and can be built upon when the system is in full use, they can be modified or split into more specific roles. The roles, like Student and Faculty, would be designated which computers/subnets they are authorized to use. For example, the Student could use both the classroom and lab computers, but not the faculty computers. For authentication in our network, the person needs to prove their identity with something they know, and something they have. This will be their password and two-factor authentication.

Firewall policies and implementation

Given our needs, we selected the Cisco Firepower 4112 Series Firewall. This solution is good for our needs and it has the scalability for future needs. This will be set to monitor all the traffic coming in and out of the network through one physical location as well as logical locations for placing firewalls. The placement will be in line with a Screened Subnet setup for our demilitarized zone covering our servers and providing protection that was not in place before. Previously unknown connections or connections from outside our network will be routed

through our external filtering router. This along with the accompanying policies will make usage of our network much safer for trusted internal users.

These firewalls will also need specific security-focused policies implemented to increase security on our network. It is useful to know that this Cisco firewall is a hybrid firewall (Next Generation Firewall) which has elements from multiple different types of firewalls. We can shape the policies needed for our network, such as blocking specific known harmful IPs. These firewalls will be set to monitor the network and its traffic patterns. The firewalls will be tailored to allow authorized traffic across the network. We will set up our firewalls for dynamic packet filtering to allow our system to dynamically react to events and create real-time rules for itself to follow. Some policies that will be in place for the firewalls will be: All traffic from within our network SCB.odu.edu is allowed out. The firewall will not be able to be accessed from the public-facing network. All data that cannot be verified will be automatically denied.

IDS policies and implementation

Additionally, the Cisco Firepower 4112 Series Firewall can also function as a location for the IDPS to function. It will be implemented around our firewall architecture with internal monitoring locations set at different points in the network. Its policies will be set for it to monitor the network at all given times. It will be set to test the state of the system periodically, as well as to measure all areas of our network. Our threat detection method will be set to anomaly-based to give us insight into anomalous issues on the network. This will allow our security team to receive alerts of unauthorized activity on our network. The IDPS we have selected will be the Cisco-integrated aWIPS IDPS. This IDPS can sit on existing Cisco systems like the edge router we have selected and we will be able to deploy it across our network, hopefully meshing with the other Cisco products.

Host Hardening policies and implementation

Host Hardening is the policies and configurations made to a system to make it more resistant and complex to attack. Many configurations can be changed on a default system because the system starts with all of its available options ready to go, but once their purpose has been determined they no longer need all of the available configurations. It is these unconfigured properties that unintentionally give attackers potential attack vectors on our network.

The original network configuration likely did not have this done to its systems. This leaves things open to more attacks than if it was configured. For example, many systems no longer use the telnet port and if you leave it open it becomes an attack vector that an attacker could use to launch an attack on the system. If the server on the network is also not hardened it is likely that the ICMP port is not blocked which opens the server to random ICMP pings and the

DoS attack ICMP Flood, which is where a server is sent so many ICMP pings that it is no longer able to serve actual requests. These are just a few examples of what could happen if a system remains unconfigured.

In our network, we will put policies in place to harden our systems and create a more secure network. We will determine the necessary ports that each of our systems needs to function and make note of all of the ports that will see no use and disable them in the systems. This is a step that will be extremely important for our important systems, like the web server and NAS. Not just the ports will need configuration, but the policies will as well. Items like password strength, enforcing a periodic update schedule, and many other policies all affect the 'strength' of a system and the network as a whole. The policies will be based on NIST recommended guidelines for effective security policy.

Software Security

First, configuring who can install what on the network systems is most important. Based on our roles that are defined, Our IT administrator and IT personnel should be the only ones who can install all applications and other systems on the network. Faculty members will be limited on what they can install to a list of pre-approved software, users or students on the other hand will not be able to install any programs or software on the network. This ensures that the network will remain secure and no unauthorized users may install software that could affect the network.

To make sure that the network is as secure as possible it is a good idea to utilize an anti-virus software to catch any of the attacks missed by the other security appliances. What we are going to do is use a product from a well-known company Bitdefender, which is known for its antivirus software which performs well in commercial use. This software will sit on every system in the network to provide protection to each of them and will send all of their data to a specialized management panel for the administrators to view and take action on.

Data Protection Measures

Data protection measures including policies, technology, backup storage locations, and restoration/recovery measures.
The protection of our data is essential utilizing the systems in place, we can use policy and other controls to ensure that our data is protected, even from unforeseeable issues. Policy to backup our data on a set interval of time to a local backup storage will provide us with needed backups of our network and its information. Tying in with our created Incident response and disaster recovery plans, our data is backed up on a set schedule and stored safely to be able to recover from incidents. All of this will also be talked about in-depth in any Disaster Recovery plans made.

Risk after Implementation

After the implementation of our controls, both on the organizational side and the physical network side, we need to re-examine our risk levels

	Asset 1 DMZ	Asset 2 servers	Asset 3 Routers	Asset 4 Domain Controllers	Asset 5 Computers
Threat 1 Software Attacks	T1V1A1 T1V2A1 T1V3A1	T1V1A2 T1V2A2 T1V3A2	T1V1A3 T1V2A3	T1V1A4 T1V2A4	T1V1A5
Threat 2 Espionage/ Trespass	T2V1A1 T2V2A1 T2V3A2	T2V1A2 T2V2A2 T2V3A3	T2V1A3 T2V2A3	T2V1A4	T2V1A6
Comprimises to intellectual property	T3V1A1 T3V2A1 T3V3A3	T3V1A2 T3V2A2	T3V1A3	T3V1A3	T3V1A4
Threat 4 Information extorsion	T4V1A1 T4V2A1	T4V1A2	T4V1A3	T4V1A4	T4V1A5
Threat 5 Sabotage/ Vandalism	T5V1A1	T5V1A2	T5V1A3	T5V1A4	T5V1A5
Threat 6 Theft	T6V1A1	T6V1A2	T6V1A3	T6V1A4	T6V1A5
Threat 7 Technical Hardware Failure	T7V1A1	T7V1A2	T7V1A3	T7V1A4	T7V1A5
Threat 8 Human error	T8V1A1	T8V1A2	T8V1A3	T8V1A4	T8V1A5
Threat 9 Quality of service deviations	T9V1A1	T9V1A2	T9V1A3	T9V1A4	T9V1A5
Threat 10 Forces of Nature	T10V1A1	T10V1A2	T10V1A3	T10V1A4	T10V1A5
Threat 11 Technical Software Failures	T11V1A1	T11V1A2	T11V1A3	T11V1A4	T11V1A5
Threat 12 Technological obsolescence	T12V1A1	T12V1A2	T12V1A3	T12V1A4	T12V1A5

With our updated controls, we can see that risk is majorly downgraded across the components of our network. Components like the firewall can help reduce the risk of software attacks, network trespass, theft, and many of the other categories. The measures we have taken have significantly reduced the risk imposed on our network.

Cost-Benefit Analysis: Several financial figures for several of our products are either non-public or deviate significantly across multiple platforms. However, to assign a total cost to our efforts we have gone through and attempted to calculate the value of our additions. The Cisco Firepower

4112 series is generally about $6700. The next appliance, the Catalyst 8300-1N1S-6T is the first item with several major discrepancies in price across retailers, however, it retails for around $80,000. The integrated Cisco IDPS (aWIPS) has no publicly available cost, however, according to the size of our network and the needs of our network this service should cost several thousand dollars per year. Our additional software should cost around $30000 in total, again many of the larger enterprise deals for software are publicly unavailable. In total, our direct cost for this upgrade will be around $130,000.
In direct comparison to what it could cost the university if personal information gets compromised, or the network around Strome is taken down for days, This amount along with policy changes and organizational changes goes a long way. The changes we made, while expensive additions for a single building

IR and DR plans

The creation of Incident Response and Disaster Recovery plans are essential to the continual running of our network. If an event threatens the confidentiality, integrity, or availability of our assets, and it has a realistic chance of success, this will then become classified as an adverse event that may affect our network. In order to bring our plans and organization into compliance with NIST SP800- we must follow a set of steps for our plan to include. The creation of both the computer security incident response team as well as the Incident response team. These teams will need to have the access and training to be able to carry out the recovery plans. These policies will include instructions on how to identify and respond to threats, restore essential functions on the network, how to recover data from storage, and how to assess the actions taken to improve for the next scenario.

The incident response plans revolve around three main actions. Detection of any threats or anomalies, understanding and reacting to them, and recovery. Utilizing the systems we have in place, such as the IDPS and some of our other tools, our teams will potentially be able to monitor and detect a threat, alerting the incident response teams and key personnel ahead of time and giving them time to prepare. The next section is Reaction, this section of the plans will detail how our teams will utilize the tools available to start handling the threat. The main goal is to quickly contain and eradicate any unwanted threats. Lastly, recovery is where our teams must, asses the damage caused by the incident, identify any vulnerabilities used, return the systems back to normal, and to document every occurrence surrounding the threat.

The Disaster Recovery plans focus primarily on re-establishing operations at Strome after a severe incident takes place. These plans revolve around several different steps: Recovering information assets that can be utilized again from Strome should a large destructive event occur. The purchasing and replacement of information assets and equipment to be able to run operations. Finally, reestablishing regular functional assets at Strome, or even at a new site if the damage is too great.

Bibliography

Whitman, M. E., & Mattord, H. J. (2022). *Principles Of Information Security.* (7th ed.). Cengage Learning Custom P.

Serversupply. (2024). *Cisco C8300-1N1S-6T Catalyst Router*. ServerSupply.com. https://www.serversupply.com/NETWORKING/ROUTER/6%20PORT/CISCO/C8300-1N1S-6T_352430.htm

Shop. (2015). Insight. https://www.insight.com/en_US/shop/product/FPR4112-NGFW-K9/CISCO+SYSTEMS/FPR4112-NGFW-K9/Cisco-FirePOWER-4112-NGFW---security-appliance/

Appliance specifications of recommended items:

Firewall/IDPS: Cisco Firepower 4100 Series Cisco Firepower 4112

- -Firewall Throughput 19 Gbps
- -IPS throughput: 19 Gbps
- -IPSec VPN throughput: 8.5 Gbps
- -Maximum VPN peers: 10,000

Routers: Catalyst 8300 Series Catalyst 8300-1N1S-6T 1 rack unit, 6 x 1G WAN

- -10G IP throughput
- -2G SD-WAN throughput
- -4 x RJ-45 + 2 x SFP embedded ports, up to 1G WAN
- -Dual power supplies