Strome College of Business Network Infrastructure Design

Toan Le, Marcos Luchetti, Hudson Sewordor

Old Dominion University

IT 417: Management of Information Security

Professor Vijay Kalburgi

December 8, 2021

Contents

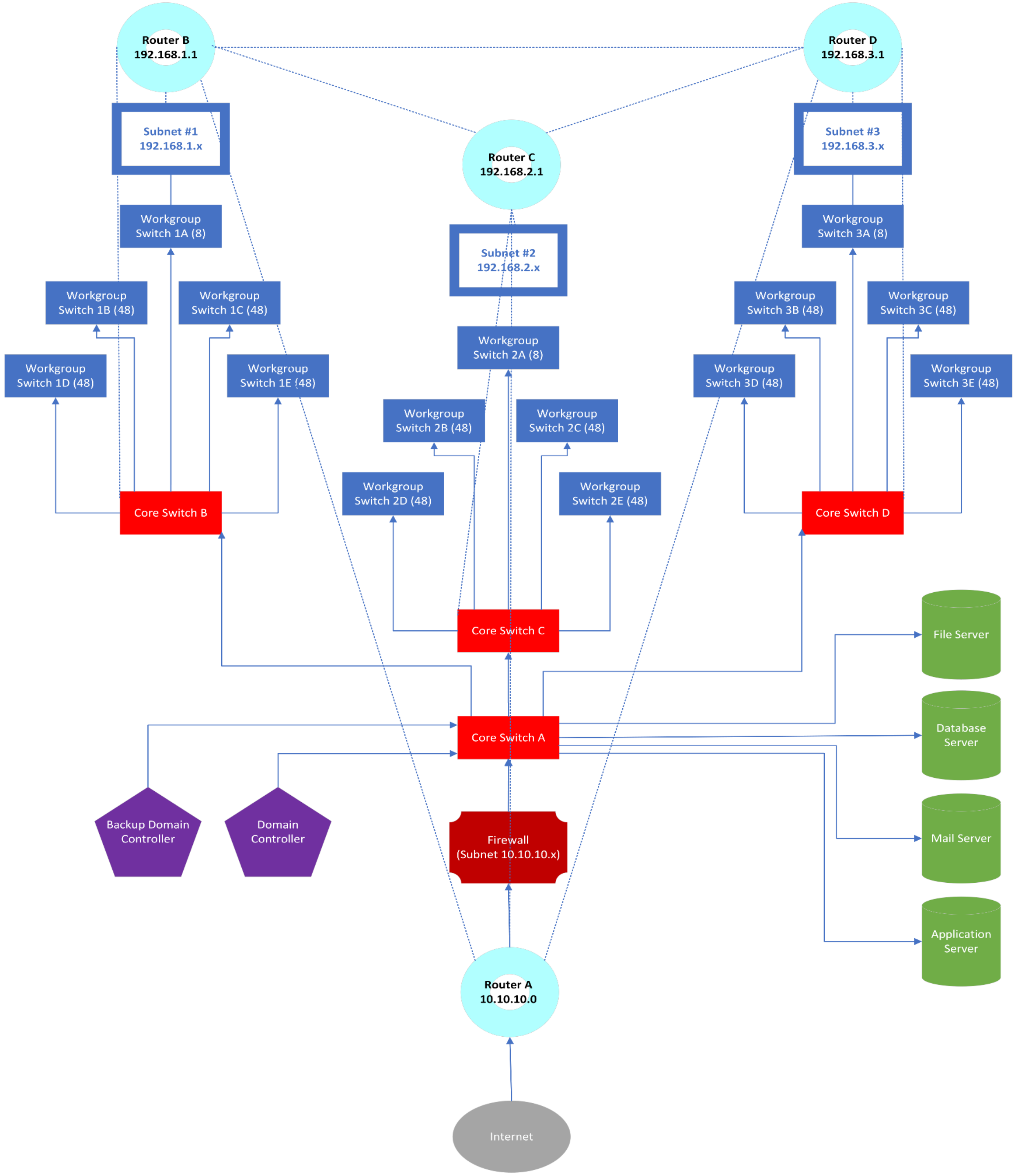
Introduction (by Toan Le, Marcos Luchetti, and Hudson Sewordor)

Every organization, government/business entity, or institution has sensitive information it wants to protect. The mission of this network infrastructure is to provide the confidentiality, integrity, and availability of the information that resides on the Old Dominion University Strome College of Business network and information assets. For instance, student education records are especially vital pieces of information for the university. As per the Family Educational Rights and Privacy Act (FERPA), these records include information such as date and place of birth, parent(s) and/or guardian addresses, grades, test scores and other academic information, disciplinary records, medical and health records, and personal identification codes, social security numbers, pictures, or other personally identifiable information that belongs to a student (National Center for Education Statistics, 1997). This report contains the design for a secure network for the Strome College of Business. The network is to be under the domain of SCB.odu.edu, and it must contain three wired subnets for labs, classrooms, and faculty offices. There will be 200 computers in each subnet, all running Microsoft Windows software, including the Windows 10 operating system, Office suite, etc. The internal network will also use private IP addresses. Finally, the network infrastructure will use Microsoft and Cisco products. This report further details each of the measures taken to provide information security, including: possible threats and attacks faced by the network; planning, organization, risk analysis, and policies; encryption and VPN techniques used to ensure confidentiality and authenticity; access control policies and implementation; firewall policies and implementation; intrusion detection systems policies and implementation; host hardening, including update policies and implementation; security for software/applications (including web based), as well as policies, configurations, and what and who may install software; data protection measures including policies, technology, backup storage locations, and restoration/recovery measures; and, lastly, incident response plans and disaster response plans.

Each of the three subnets will have 200 computers, which means that there are 600 computers that need to be connected to the network. This calls for acquiring networking hardware, which includes switches, routers, domain controllers, and servers. Twelve CISCO DESIGNED Business CBS350-48T-4G and eight CBS350-8T-4G switches will be used to provide Internet for these 600 hosts and three routers. There will be four Cisco Catalyst 3750X-12S-E core switches, each connected via ethernet to its respective router. Routers will be used to connect the different subnets. For that, four CISCO C921-4P routers will be configured to forward packets between each subnet. The network will have four servers: an application server, mail server, file server, and database server. The Cisco UCS® C480 M5 Rack Server will be used for file storage. Five Cisco UCS C240 M6 Rack Servers will be used for the database, mail, and application server, as well as for the Active Directory server and its backup server. As for the firewall appliance, the CISCO FPR-1120 will be able to support the Strome College of Business' 600 computers. This device provides threat defense software, which includes Firewall (FW), Application Visibility and Control (AVC), and an Intrusion Prevention System (IPS). In addition, this firewall supports 200K maximum concurrent sessions and 15K maximum new connections per second. This firewall appliance offers the right balance between protection and cost for the needs of the college, and its wealth of features makes it future-proof for several years. The next component to the network is the domain controller. The main function of the controller is to respond to a request such as an authentication alert to verify users on the domain network. These controllers are used to maintain and organize data that goes in and out of the network. This is what we call the Active Directory which is a database that stores objects of users and computers. This also acts as a secure way to manage the policies of Windows NT and Windows Server. Within a network server there only needs to be one domain controller. But in the case that the controller shuts down abruptly, all data stored could be lost without retrieval. For larger businesses, it would be best to have a second domain controller in an event that one fails. If a network decides to obtain a single domain controller, there is a potential loss of directory services which contains user logs. There would also be a loss of DNS, which would be having the ability to search for resources whether it be locally or externally. For that reason, having two domain controllers ensures the stability and reliability of the network to function.

The network diagram on the next page shows how the network will be set up using core and workgroup switches, routers, a firewall, a domain controller with a backup, as well as file, database, application, and mail servers.

Figure 1. Internal Network Diagram (by Marcos Luchetti)



Possible Threats and Attacks (by Toan Le)

Network security has become one of the main reasons cybersecurity and infrastructure are continuously trying to handle the development for the protection of online information. These flaws can stem from most commonly software attacks but also hardware and other organizational systems. These vulnerabilities that are exploited could become detrimental to the organizations by exploiting sensitive data such as customer address, name, and phone number. Some companies that also require more data such as social security can be a serious problem when it comes to data security. As time continues and the pace of technology rapidly improves there are a larger number of workers that are working from home. These network protections must be at an all-time high along with infiltrators who seek chances to find data.

One of the most common network threats is the Distributed Denial of Service, also known as DDoS. This type of attack makes online series unavailable by sending requests to the service with traffic so the website would stop functioning. This could happen to websites such as businesses which in turn could stop them from selling products.

Other common viruses that are faced amongst users every day are viruses and worms. These are most commonly affecting users by malware being installed on the computer through links or downloads that the user may have clicked on. These types of attacks on the network can be serious as they could affect the system by bringing irreparable damage. Some of these viruses the people encounter may not have a direct effect that users can see but can run in the background and retrieve information such as emails, usernames, and passwords.

Ransomware has also become a fear amongst the network attacks that occur. This type of attack encrypts data stored on the system and in return, a ransom demand is sent out. In the ransom, if not fulfilled. then sensitive files could be permanently deleted. People find this fearsome and end up paying the ransom. Large corporations that also encounter this have also lost a large amount of money. This type of software continues to evolve and become a part of the network obstacle that cyber specialists try to prevent.

As for the biggest threats for networks they are Botnets. Several interconnected devices are used for running multiple bots. This type of threat is used for remote-controlled attacks on a network. An attack is typically launched through spam emails to create fraud or data theft. These types of attacks are also in place to force users on the end to pay a ransom to regain access back to either their files or control of the system.

The development of technology rapidly evolving causes more problems to arise. Network security attacks tend to be more apparent. An ideal situation where one can identify the problem and initiate a plan to prevent it would stop attacks from doing further damage. There are more security measures taken in place to reduce the risk of encountering such problems with network attacks.

Planning, Organization, Risk Analysis, and Policies (by Marcos Luchetti)

Once all possible threats and attacks faced by the network are identified, the next step in the risk management framework is to perform a risk analysis and then create policies that address the current level of risk. The plan involves cooperation from all communities of interest, that is, the information security (InfoSec) community, information technology (IT) community, general management, and users. The InfoSec community will lead in addressing risk to information assets, since they are most knowledgeable about threats and attacks that could harm the college's information assets. The IT community will be responsible for the building and safe operation of secure systems. General management and users must be trained and aware of the threats against the organization. In addition, management must also make sure that InfoSec and IT have adequate time, money, personnel, and other resources to meet the organization's security requirements. Together, all these communities of interest must work with one another to address all areas of risk, from the most devastating of security breaches to the slightest user mistakes. The InfoSec, IT, and general management teams are responsible for evaluating current and proposed risk controls, determining which control options are cost-effective for the organization, acquiring/installing the needed controls, and ensuring that the controls remain effective (Whitman & Mattord, 2021, p. 125).

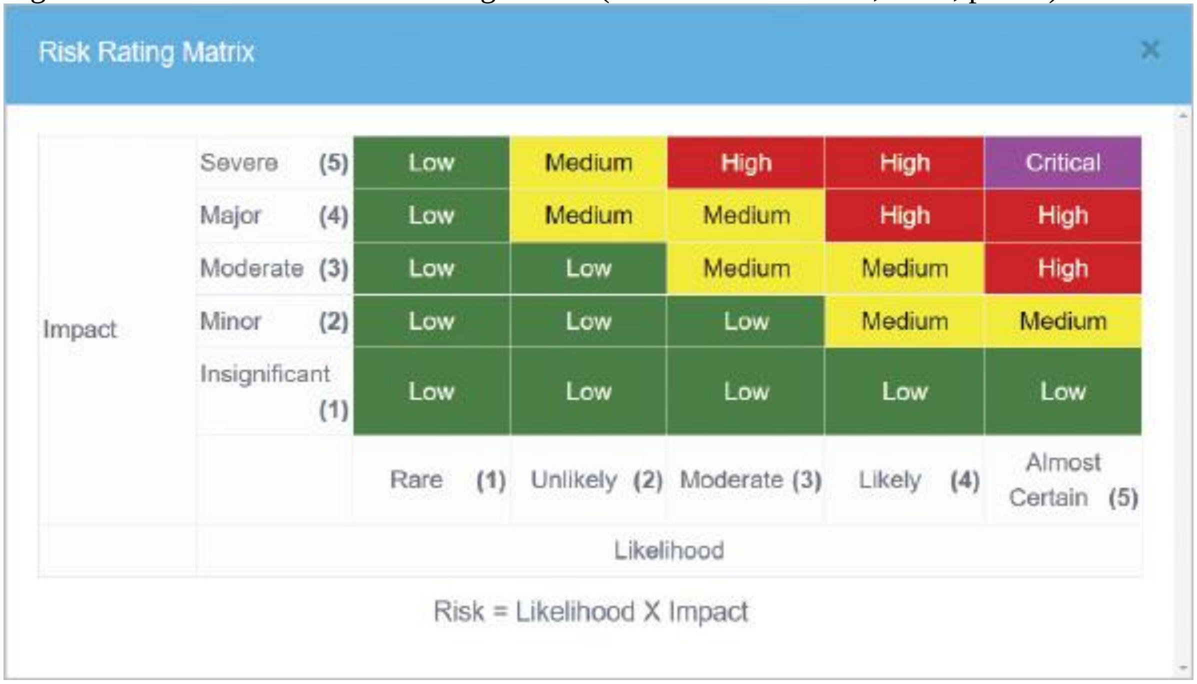
The three communities of interest must acknowledge the constantly evolving landscape of threats to the confidentiality, integrity, and availability of information assets. To address this concern, there must be periodic managerial reviews/audits of these groups and their mitigation strategies/techniques. For general management, this would also involve providing oversight and access to information that is stored outside the IT department. Moreover, general management is responsible for keeping a routine inventory of the college's assets. And, through IT audits, ensure that the asset inventory is verified for completeness and accuracy. Then, the InfoSec and IT communities must review and verify threats and vulnerabilities in the asset inventory, also assessing the current controls and mitigation strategies. They must then perform a cost-benefit analysis of the controls, also determining if the decisions they had made for deploying the controls are still valid and if the controls should be changed or not based on this assessment. General management must frequently verify each control for its effectiveness. To ensure that no information asset is at risk, managers may ever so often walk through the labs, classrooms, and faculty offices after work hours, checking that confidential information is secure, workstations have been shut down, users are logged off, and ensuring that trash cans do not contain sensitive information that was tossed away. Other controls to be put in place include following policy, promoting training and awareness among students and faculty, and employing appropriate technologies (Whitman & Mattord, 2021, p. 125).

The management's intent for the outcome of the college's effort to maintain confidentiality, integrity, and availability of information assets is to be outlined in the policy. This policy will provide guidance that forms and governs the risk management efforts in the college. The risk management (RM) policy must have a clear and identified purpose and scope, RM intent and objectives, roles and responsibilities, resource requirements, risk appetite and tolerances, RM program development guidelines, special instructions and revision information, in addition to references to other key policies, plans, standards, and guidelines (Whitman & Mattord, 2021, p. 126). The framework team and the process team must be assigned with specific tasks once the framework itself has been designed and gone through at least one iteration. Then, the framework team will mostly be responsible for overseeing the RM process, instead of developing the framework. The framework team must also draft a risk management plan, which specifies the college's risk appetite, or what risks the institution is willing to bear. The college's risk appetite is likely to influence RM planning. Prior to development, the plan must be distributed to all mid- to upper- level managers for a desk check prior to being implemented. After that, the plan must go through pilot-testing, where it is deployed in a small area to find any pros and cons before being fully adopted. Once adopted, the RM plan must be continuously monitored, communicated, and reviewed by the RM framework team, to detect and address issues before they become serious threats to the program.

With the guidance of the RM plan, the RM framework will then undergo the implementation phase. It is during this phase when risk evaluation and remediation of key assets must be carried out. As stated earlier, the three communities of interest (InfoSec, IT, and general management) must cooperate with each other to address all levels of risk. By having representatives from each community of interest come together to collaborate and assert themselves in RM process activities, they can start establishing the context of the program, identifying risks, analyzing risk, evaluating risk, treating risk, and exploring methods to further mitigate risk (Whitman & Mattord, 2021, p. 128). Earlier in this report, we established the context and identified possible threats and attacks faced by the network. Risk analysis will help to determine the likelihood that vulnerable systems will be attacked by specific threats, in addition to assessing the relative risk facing the organization's information assets, allowing risk management and control activities to focus on assets that need the most immediate attention (p. 128). Risk analysis also includes calculating the risks found in assets whose current settings indicate vulnerabilities, as well as observing controls that may have an impact because of identified vulnerabilities and ways to mitigate risk (p. 128). The findings discovered during risk analysis must be documented and reported.

In the risk analysis process, a risk rating or score will be assigned to each specific vulnerability, enabling you to measure and compare the relative level of risk of certain information assets. Something like the Clearwater IRM risk questionnaire form pictured below can be used for risk analysis. This tool makes use of several risk questionnaires to analyze the threats and vulnerabilities of information assets. Moreover, there should be a risk likelihood scale to determine the likelihood that a certain vulnerability will be exploited or attacked—the higher the number, the more likely the event is going to occur. For the Strome College of Business, here are some examples, using a scale of 1-10: the likelihood of network infiltration (8), malicious insider event (6), accidental exposure of sensitive information (5), fires (3), hardware failures (2). The next step in risk analysis is to assess the potential impact or consequences that a successful attack would have on asset value. The goal is to reduce the amount of loss of value of an asset, and, as such, the focus of the school should be to focus its protection efforts on the value of these assets. This is where the weighted tables, which assign value to assets and are used in risk identification, become handy. It would also be a good idea to be on the alert on successful attacks that happen in other institutions and organizations. To better understand the potential impact of a successful attack, the institution can create worst case/most likely outcome scenarios by taking a particular threat and speculating on the worst possible outcome of a successful attack, and then determine the most likely outcome. A risk impact value could then be assigned to each scenario (much like the one used for risk likelihood). For example, the Strome College of Business could use a scale of 0-10, assigning each rank to a certain scenario, also including the number of records at stake, productivity hours lost, and financial impact. It would be wise to share this information with the contingency planning management team, as it will help them understand how the organization needs to respond to a successful attack and plan for incident response, disaster recovery, and business continuity, which would save much time and effort (Whitman & Mattord, 2021, p. 143). After finding risk likelihood and impact, the next step in risk analysis is risk determination, or the quantification of certain risk elements by using this formula: Risk = Likelihood × Impact ± Element of Uncertainty (if you wish to simply accept the uncertainty factor, then opt for the simpler formula Likelihood × Impact). For instance, there are 200 workstations in each of the three subnets in the Strome College of Business–let's assume that this has a risk impact value of 10–and say there is a threat of network infiltration, which is ranked at 8 on the risk likelihood scale. Assuming that the assumptions and data are 90 percent accurate, with an uncertainty of ± 10 percent, the resulting risk rating is 80 ± 8, so the resulting risk rating range is 72 to 88 on a 100-point scale. Below is an example of the IRM Risk Rating Matrix within the range of 1 to 25:

Figure 2. Clearwater IRM Risk Rating Matrix (Whitman & Mattord, 2021, p. 143)



Risk Rating Matrix

Impact	Severe (5)	Low	Medium	High	High	Critical
	Major (4)	Low	Medium	Medium	High	High
	Moderate (3)	Low	Low	Medium	Medium	High
	Minor (2)	Low	Low	Low	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
	Likelihood					

Risk = Likelihood X Impact

The risk rating worksheet is another useful document that can be used to calculate risk vulnerability for information assets, ignoring uncertainty altogether (essentially Likelihood × Impact). The worksheet lists assets, vulnerabilities, likelihood, impact, and risk-rating factors. The information in this worksheet demonstrates the identification of assets as they are matched with vulnerabilities, as well as assessing the relative risks for each pair. The most important pair will then be identified as the one that would most improve the security of the institution once repaired. An example of the worksheet for an organization is shown in the below table:

Table 1. Risk Rating Worksheet (Whitman & Mattord, 2021, p. 143)

Asset	**Vulnerability**	**Likelihood**	**Impact**	**Risk-Rating Factor**
User service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
User service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
User order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
User order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20

Encryption and VPN Techniques (by Hudson Sewordor)

A Virtual private network (VPN) will be used as an advanced telecommunications infrastructure in order to create a tunnel for private communication. The goal and use of VPNs are mainly to allow internal network connections within the organization to travel securely to remote locations. Trusted VPNs will conduct packet switches over leased circuits that work with the service provider. The service provider is responsible for giving the organization contractual assurance that the circuits provided will be safely protected from outside interference and maintained properly only to be managed by the organization. Security protocols such as IPsec will be used by Secure VPNs to help encrypt traffic transmissions that are transmitted over the internet and other public networks (Whitman & Mattord, 2021, p. 139).

The Hybrid VPN is made of a combination of both the secure and trusted network versions. The Hybrid version will likely be the most beneficial network to ensure secure travel of communication weather being transmitted privately within the organization or over public networks. For the VPN to run at the highest form of efficiency it will be able to encapsulate data that is input and output it. The network will be able to navigate the embedded client within the allocated parameters of the protocol. The protocol is then routed over a public network that can be used by the server (Whitman & Mattord, 2021, p. 139).

The VPN will also be able to run an encryption of the incoming and outgoing data. This ensures that the content of the data will be kept private while being transmitted over the network. The data can still be used by the client and server computers as well as other local networks that are on either end of the VPN connection. The final goal that must be achieved by the VPN is the ability to authenticate both the remote user and computer. Both authentication and subsequent user authorization are used for specific purposes predicated towards having an accurate identification for both the remote system and the user (Whitman & Mattord, 2021, p. 139).

Access Control Policies and Implementation (by Toan Le)

For access control policies, high-level requirements are made so that only certain people would have access. These policies show that the scope where it applies would be to the employees, contractors, users, and customers. The limitation that signifies only certain access control policies would apply. This typical role for a control policy manages the resource of the company and how it is used. The scope of this section is to signify if the access control policy applies to one or not.

As for the Purpose, this minimizes the potential exposure from unauthorized use and allows for information to stay protected. The role of this is to state the goal to protect sensitive information and resources. It is important to make this clear as people should know what exactly is being discussed and how the policy wants to move about it. This decreases the chance of people misinterpreting the information and understanding how it may apply to one.
Reducing the risk and unauthorized access as well as protecting the integrity of the network are common goals the information security policies mainly include.

The Responsibilities standing are duties amongst a team that has no absolute control over but are there so that teams in place would work together to monitor the systems. This decreases the chance of having an individual committing any mistakes. From this section, knowledge of how access controls are implemented and how it differs from other parties make it clear that different systems require different responsibilities.

Only those who require data for a certain task would be allowed to use the resources available. As for those who don't need the data, access to the data shouldn't be allowed. This reduces the risk of leaking data and limits the number of users interacting with the data. Even with the utmost care, having multiple people access poses a greater risk. With users having access to the data, there could be a user that has this information compromised leading to a data breach in the system.

Password Policy has an established rule as to how passwords are made. In this process of creating a password, they must meet certain requirements for it to be valid. With additional letters changing from lower to uppercase and adding special characters with no formed words could be the best way to create a difficult password for hackers to get a hold on. In this policy, rules are set to prevent users from having a password exposed and keep them safe from hackers who can have a difficult time cracking the passwords.

The Adherence section highlights what could potentially occur if access control policies are breached. This process contains punishment for actions that aren't followed by the policies stated. This is why policies have been made very clear so that any type of failure to follow policy would hold a reasonable punishment for the actions done. To keep the policy in place, company reinforcement would be through repetitive training so that policies are clearly remembered and acknowledged.

In brief, for an access control policy to be effective, there must be an Implementation. It would be followed through with methods and procedures. These act as a guideline for a structure in the policies to come about.

Firewalls: Policies and Implementation (by Marcos Luchetti)

In addition to access control policies, firewall technology presents another important systems-specific security policy (SysSP) to consider. A firewall policy must have a clear statement of managerial intent, as well as guidance to network engineers for selecting, configuring, and operating firewalls. A successful firewall implementation relies not only on the firewall itself, but also on the policy which guides and regulates the way in which the firewall will respond to network traffic. This policy will provide a set of rules that the firewall will be dependent on in order to block and accept different kinds of traffic being transmitted over the network. In addition, the firewall should have an access control list (ACL) that assigns each authorized user with a certain level of access. The firewall policy below is what will be used to protect the school's network from malicious traffic that could harm information assets.

Firewall Policy for the ODU Strome College of Business

I. Statement of Policy

The goal of this policy is to implement a firewall that improves the security and reliability of the connections established between the Strome College of Business and the Internet. This firewall component is essential to the overall network security architecture of the school.

a. Scope and Applicability

The firewall policy applies to all users on the school's network, which includes faculty, staff, administrators, students, information assets (hardware and software), and networks.

b. Definitions

Firewall is a term which refers to the hardware and software technologies that prevent specific types of information from moving between two different levels of networks, such as an untrusted network (the Internet) and a trusted network (the school's internal network). The firewall may be a separate computer system (hardware firewall), or a separate network that contains several supporting devices.

Firewall Processing Modes refer to all the processing modes which are used to determine if a packet should or should not be allowed through the network. These include packet-filtering firewalls, applications layer proxy firewalls, media access control layer firewalls, and hybrids, which use a combination of modes.

Firewall Architectures are those architectural implementations of firewalls that are commonly used by organizations and other entities. These include single bastion hosts, screened host firewalls, and screened subnet firewalls.

Users are the individuals (faculty, staff, administrators, students, volunteers, and visitors) that are granted access to the school's information systems to access information technology resources.

c. Responsibilities

The information security, information technology, and general management communities of interest (CoI) are responsible for implementing and maintaining the school's firewall. They are also responsible for the activities mentioned in this policy and must give out guidance when needed. Maintaining the security of information assets requires that every employee is diligently following the best practices outlined by the security policy.

II. Firewall Configuration and Implementation

The firewall is to be used for limiting the traffic that goes in and out of the school network. Any service will be denied access unless it is expressly permitted. All users must be authenticated and verified.

a. Packet-Filtering Firewall Procedure

This type of firewall will examine the source and/or destination IP address for each packet, as well as the type of transport protocol for each packet (for example, HTTP, FTP, telnet, etc.).

- For inbound traffic, the packets coming from essential services will be accepted because they are needed for certain activities, subnets, hosts, applications, or users; all other packets will be discarded
- For outbound traffic, packets will be allowed to be sent to hosts and services outside the school's trusted internal network; traffic going to vulnerable hosts and services will be blocked to prevent any malware from spreading throughout the network
- Permitted services include E-mail Servers, Web Servers, Blackboard, IT Helpdesk, Remote Desktop, Library Services, and University Services
- Prohibited services include Malware-Related Protocols; all data that is not verifiably authentic should also be denied

b. Protocol Access

The following list contains specific instructions for the common protocols that are used to transmit data over the network:

- Simple Mail Transfer Protocol (SMTP) (port 25) data may pass through the firewall, but it is routed to a SMTP gateway to filter and route messaging traffic securely
- Internet Control Message Protocol (ICMP) data is prohibited from entering through the firewall to prevent snooping by hackers (only allowing internal administrators and users to use ping)
- Telnet (port 23) access must be blocked on all internal servers from the Internet to prevent illegal zone transfers and to prevent attackers from taking down the network
- File Transfer [Default Data] (FTP) (port 20) and File Transfer [Control] (FTP) (port 21) should be blocked because they are vulnerable and obsolete
- Network Time Protocol (NTP) (port 123) should be blocked due to attackers' propensity to abuse NTP servers into carrying out DDoS attacks on machines
- Domain Name System (DNS) (port 53), Hypertext Transfer Protocol (HTTP) (port 80), Post Office Protocol version 3 (POP3) (port 110), Simple Network Management Protocol (SNMP) (port 161), and Hypertext Transfer Protocol Secure (HTTPS) (port 443) are allowed because they are used by essential services

Assuming that the destination address of the internal network is 10.10.10.0, and that the 10.10.10.1 and 10.10.10.2 addresses regulates external and access respectively to and by the firewall, the below table shows a list of rules for the configuration of the firewall based on the information above:

Table 2. Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.1	Any	Deny
2	Any	Any	10.10.10.2	Any	Deny
3	10.10.10.1	Any	Any	Any	Deny
4	10.10.10.2	Any	Any	Any	Deny
5	Any	Any	10.10.10.0	>1023	Allow
6	Any	Any	10.10.10.0	7	Deny
7	Any	Any	10.10.10.0	20	Deny
8	Any	Any	10.10.10.0	21	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.0	25	Allow
11	Any	Any	10.10.10.0	123	Deny
12	Any	Any	Any	Any	Deny

c. Implementation

Below are the guidelines for the implementation of the firewall.

- The firewall must reside on dedicated hardware. The host machine must not run any applications that could compromise the firewall’s security and effectiveness.
- There must be a record of the initial build and configuration of the firewall, to establish a baseline, track any changes, and maintain the current state.
- In the event of hardware/software failure of a firewall component, all traffic going in and out of the network will be blocked until the problem is resolved.

Only firewall system administrators are permitted to logon to the firewall.

- Firewall hosts can only be accessed by firewall system administrators
- Root access is only accessible via personalized logon; it cannot be accessed remotely

Only authorized personnel can change firewall access rules, software, hardware, or configuration.

- There must be a record of any changes made to the firewall.
- There must be a valid reason for changing the firewall configuration.
- The three communities of interest must continuously keep track of what ports are required to meet the school's needs.

The firewall system must alarm InfoSec personnel whenever an incident occurs.

- Response to such events must be in accordance with documented procedures made for these situations.
- There will be certain security events which are to be dealt with automatically by the firewall system.
- If an attacker is attempting to penetrate the firewall, network services must be temporarily shut down until the threat is dealt with.

III. Firewall Security/Policy Review and Modification

Below are the guidelines for the testing of the firewall, as well as for the review of firewall security/policies and the means for conducting modifications to firewall security and/or policy.

a. Firewall Security Testing

There must be routine testing of the firewall. Testing must be done to find errors in the firewall, including:

- Firewall configuration errors showing exploitable vulnerabilities
- Firewall rule set inconsistencies to match the desired state
- Firewall host and application integrity

b. Firewall Security Audit

There must be regular auditing/logging to ensure that there is a record being kept of firewall activity.

- Logs must be kept so that firewall activity can be analyzed. This information may prove useful for determining the cause of a security event and where to address the holes in security.
- All traffic must be logged in order to detect suspicious activity.

c. Scheduled Review of Policy Procedures

The definitions, practices, and technological factors in the policy must be reviewed annually to ensure that the policy is effective and up to date. If there is a major change to the networking needs of the Strome College of Business, the firewall security policy may be changed to meet the requirements.

d. Procedure for Requested Modification

People are allowed to make recommendations for revisions of the policy via e-mail, office mail, or anonymous drop box. When the time comes for review of the policy, all submitted comments will be examined, and management-approved improvements should be implemented.

Intrusion Detection Systems: Policies and Implementation (by Hudson Sewordor)

Intrusion detection systems will be put in place with the goal of preventing outside attackers from gaining access into the organization's information systems. When outside attackers gain access to the organization's infrastructure, they may be able to disrupt the normal operations of the organization. Attacks may vary depending on the intent of the attacker. Some attacks may be made anonymously, where the intruder's goal is to cause harm without leaving a trace or the ability to identify them. While other intrusions are done so notoriously, leaving an imprint on the harm they were capable of committing when accessing the organizations systems (Whitman & Mattord, 2021, p. 338).

It's important to determine when an intrusion is being committed. Some other interfering incidents may occur that may not qualify as an intrusion but may still have the ability to disrupt the performance of the organizations. These threats may be unpredictable, varying from internal issues such as system service outages, to world issues such as natural disasters occurring.

The prevention systems will be implemented in order to deter and avoid the possibility of an intrusion occurring. The intrusion detection system operates like a surveillance alarm. It has the ability to detect abnormal behavior or activities that may be lurking. The system will use an alert messaging system notifying the administrators via email or SMS text message of fraudulent authentication or possible breaches occurring. Other signaling features such as a sound alarm, visual light blinkers, or vibration patterns can be managed to alert the admin and its operators of a break-in occurring. The administrators may also configure the system's alarms to specific alerts in order for them to determine the severity of the attack that may occur (Whitman & Mattord, 2021, p. 339).

Network based Intrusion Detection systems are built of both hardware and software appliances in order to monitor and direct network traffic. Agents are installed on other segments of the network to monitor possible intrusions remotely. The NIDPS is programmed to be able to identify traits and patterns made by intrusion activity. The NIDPS also examines packets within the network traffic monitoring familiar connection request packets which is key to determining whether a potential attack is going to occur. The NIDPS sensors are installed within the router where they are able to monitor incoming and outgoing traffic. It can also be deployed to monitor specific computers on a network segment. NIDPS compares measured activity to specific signatures that are in the system's knowledge base (Whitman & Mattord, 2021, p. 343).

Host Hardening and Updates: Policies and Implementation (by Toan Le)

In the field of computer security, host hardening has many different meanings such as shutting off-network services by firewalling. The main purpose of host hardening is to protect and provide layers of protection. It also has the meaning of allowing existing services to only be available to certain users at a specific time. This states that users only have limited access, if necessary, in which the level of access would be prioritized to be higher.

The process of host hardening begins with removing unused applications. On the majority of devices, many services are running in the background that many don't know of. For there to be a server installation, some requirements may go as there aren't any user necessary applications. It is also necessary to keep the system up to date. Some patches are continually sent out for security purposes. Keeping this updated would have fewer encounters with issues. All updates sent out are patches that stop errors or vulnerabilities from becoming a potential threat. Using software like smart deploy is great for keeping backups or copies of the system files in the case of a failure with the system.

The need to frequently check who and what is accessing the service is crucial to keep an eye on users and their activities. Controlling the network service would allow you to be alerted when someone is trying to access unrestricted areas of the network. Open source like port scanners can be used to scan vulnerabilities and identify what devices and hosts are on the system which could detect security risks.

It is also emphasized that it is necessary to disable windows services and ports at all costs. Some of these Windows services contain IP addresses and registered names. Disabling remote services such as the terminal services are due to unencrypted services that could pose a potential threat where eavesdropping attacks could be initiated.

Some elements of host hardening include physical security, installation and configuration, fixing vulnerabilities, and disabling unnecessary services. The issue that comes from these factory systems is the vulnerabilities that have already been in place in the system. After removing these services, the system becomes hardened in which there are complex processes that become involved to create a secure service.

The security baseline for these systems needs system administrators to manage several servers and for admins to maintain several servers. Standard configurations for PCs could pose restrictions. Some applications, configuration settings, and interfaces are restricted due to software interference. Ensuring that the software is configured safely and enforcing policies is important as for maintenance costs which makes it easier to diagnose errors.

Policies that have been applied in this group policy object consist of consistency, reduced administrative custom compliance, and control. Being constant means that a security policy is applied across the whole organization. The corporate policies are also handled and applied from a single management console. Compliance comes with rules and regulations that are met and controlled to keep everything as users and systems are kept in check.

Security for Software and Applications (by Marcos Luchetti)

Software is a component of an information system which includes applications, or programs, operating systems, and a variety of command utilities. This software contains much of the vital information within an organization, or in this case, the Strome College of Business. As such, the handling of the software, which includes installation, must only be done by authorized personnel from the InfoSec and IT communities of interest. This will ensure that all software on the system is accounted for and that it was installed properly. Out of all the components of an information system, software is the most vulnerable, as software programming errors are responsible for most cyber attacks (Whitman & Mattord, 2021, p. 15). To mitigate this risk, it is essential that the university implements effective security policies and configurations for software and applications. The following configurations will provide the school with solutions that allow authenticated end users to communicate and transmit information through software and applications, Web-based or not, with the proper security, encryption, and nonrepudiation.

To promote the security of information systems, software/applications will need to use public key infrastructure (PKI) systems as a means for providing authentication, integrity, privacy, authorization, and nonrepudiation. PKI systems are based on public-key cryptosystems, and they also rely on digital certificates and certificate authorities (CAs) (Whitman & Mattord, 2021, p. 401). Digital certificates are container files that contain a key value used by the PKI system and end users to validate public keys and their owners. These digital certificates are usually issued by a certificate authority and come attached with a digital signature that certifies the file's origin and integrity (p. 403). For instance, if one of the college's computers is downloading an update from the Internet for one of its applications, such as a Microsoft Windows update, the digital certificates and signatures are there to ensure that the downloaded files originated from the source it's supposed to. A registration authority (RA) that works with the CA will be responsible for certification functions, including verification of registration information, creating end-user keys, revoking certificates, and validating user certificates.

There are a few different types of digital certificates that will be used on certain client-server applications. The Strome College of Business' Web servers and Web application servers on the SCB.odu.edu domain will be using Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol to establish an encrypted SSL session, as well as the Secure Hypertext Transfer Protocol (HTTPS), which encrypts messages transmitted via the Internet between a client and server. The Web clients on the domain will be using client SSL certificates to authenticate users, sign forms, and participate in single sign-on (SSO) solutions via SSL. HTTPS will provide confidentiality, authentication, and data integrity through different trust models and cryptographic algorithms (p. 406). Mail applications will be configured to use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms (p. 403).

Certificates must be kept safe in certificate directories, which should only be accessed for administration and distribution purposes. Management protocols for PKI systems must also be integrated. These protocols include the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information for authorized individuals (p. 401). To meet the security demands of the college, the PKI must include systems that issue digital certificates to users and servers, directory enrollment, key issuing systems, tools for managing key issuance, and verification and return of certificates (p. 401). Additionally, there are certain PKI solutions that can further limit the access to and exposure of private keys. These include password protection, smart cards, hardware tokens, and flash memory or PC memory cards (p. 401). To ensure the greatest security for these systems, end users will be required to retrieve a one-time token code from Duo Mobile on their smartphones upon logon for each session.

Lastly, Pretty Good Privacy (PGP) presents itself as another viable method for encryption and authentication of e-mail, as well as file storage applications. PGP is a hybrid cryptosystem that is based on some of the best available cryptographic algorithms. These include the RSA/SHA-1 or DSS/SHA-1 algorithms, which provide public-key encryption for digital signatures; 3DES, RSA, IDEA, or CAST algorithms, which provide conventional encryption for messages; and the ZIP algorithm, which compresses messages after they have been digitally signed, but before it is encrypted (Whitman & Mattord, 2021, p. 411). After all these encryption and conversion functions have been processed, PGP then automatically subdivides messages into a manageable stream size that does not exceed most Internet facilities' limit on message size. When the message is received by the recipient, PGP will then reassemble the segment's message blocks prior to decompression and decryption (p. 411). Public-key management is conducted through the use of a public-key ring structure. This structure addresses the problem of trust in PGP. Essentially, each specific set of public-key credentials will be associated with a key legitimacy field, a signature trust field, and an owner trust field, each field containing a trust-flag byte that determines if the credential is trusted in that field. If a key is to become compromised, and the trust of a given credential is broken, the owner can issue a digitally signed key revocation certificate that updates the credential trust bytes upon the next verification (p. 411).

As per the guidelines written out on pages 79-82 of *Safeguarding Your Technology* (1998), the college should adopt the following systems-specific security policy strategies to further promote software security:

- Keep a record of what programs are being installed, uninstalled, and changed
- Ensure that there is not any obsolete software on the systems, and that software is up to date and working properly with each other
- Test new software before full implementation
- Store critical backup copies on a well-maintained, off-site location
    - Backups include all software, databases, and information that serve critical functions
    - Backups must be always readily accessible
    - Periodically perform checkups on backups to ensure that they work as intended
- Secure master copies of software and associated documentation
- Never lend or give proprietary software to unlicensed users
- Information systems must use only licensed and approved software
- Monitor software use and hard drive contents to find unlicensed software on information assets
- Only authorized personnel are permitted to install software on information systems
- Conduct IT training for faculty and staff on the use of software and security policies
- Define security needs before purchasing new software
- Require written authorization before anyone makes changes to software

Data Protection, Backup, and Recovery Measures (by Hudson Sewordor)

A combination of both on and off-site drivers, cloud storage, and backups are used by the organization as a backup point because recent data can potentially be lost as more data is stored within the system. Redundant array disks (RAID) are implemented in order to have a safe store option for backups. The organization will also implement bulk batch transfers of data over secure internet connections. The data is then archived by the receiving end of the server. It is encouraged for an organization to have up to three copies of important data stored in both the cloud backup and local hard drive storage units (Whitman & Mattord, 2021, p. 196).

The Community policy and management team is responsible for conducting an impact analysis using scenarios and other methods in order to have certain guidelines that may be followed in the case that a disaster was to occur. The team must prioritize human resources to ensure that the people operating within the organization are well informed with the amount of knowledge necessary in the event that business operations must be restored. A clear set of roles and responsibilities must be listed so that members are aware of company personnel. An alert roster must also be included consisting of 911 departments such as medical services, police, and fire departments. Insurance agencies and other management teams will also be included in the alert roster. In the event that a disaster was to occur, it is important that all human working members of the organization are prioritized before any other working resource that makes up the organization. All employees must be accounted for before other assets of the organization may be sought after (Whitman & Mattord, 2021, p. 198).

When a disaster occurs, each action and procedure performed must be documented in order to reference later when a report is being conducted on the disaster. If primary implementations for system components are unavailable, alternative ones should be developed and ready to apply if needed. Systems that include a large capacity, auto recovery, and fail-safe features are best recommended for a quick recovery to be possible. Data recovery requires backup strategies to be flexible and adaptable to different hardware configurations in order to increase the possibility of restoration (Whitman & Mattord, 2021, p. 199).

This is why the system management is a top priority, because of how critical the methods must be able to translate over different hardware and software components. Each of these procedures and solutions will be documented in an integrated strategic plan that can be accessed when necessary. Lastly in the case of an emergency, all employees are responsible for always having emergency contact information in their possession. Personal information such as conditions, disabilities, or emergency products must be recorded. A set of instructions must also be included in the case an emergency occurs and actions must be taken. This information may be recorded on an identification card. Name, addresses, phone numbers, and emergency contacts are all types of information that may be recorded on a user's ID (Whitman & Mattord, 2021, p. 200).

Incident Response Plans and Disaster Recovery Plans (by Marcos Luchetti)

In information security, it is a well-known fact that, sooner or later, there will come a time when a hacker breaches the network's defenses. In these unexpected situations, time is of the essence. There will need to be incident response and disaster recovery plans that systematically address how to identify, contain, and resolve any possible unexpected adverse event. This is done to make sure that these information systems are able to operate effectively without excessive interruption.

It is important to note that an incident response (IR) plan is not a preventative measure, but a reactive one, although most IR plans provide preventative recommendations. The IT manager who possesses security responsibilities will be the one responsible for creating the IR plan. There will be an independent IR team composed of members from each community of interest, and the roles and responsibilities of each team member must be clearly documented and communicated throughout the organization. The IR plan must also include an alert roster, which lists certain critical individuals to be contacted during an incident (Whitman & Mattord, 2021, p. 189). The school will be following the incident response plan of action as outlined by this incident handling checklist from NIST SP 800-61, Rev. 2:

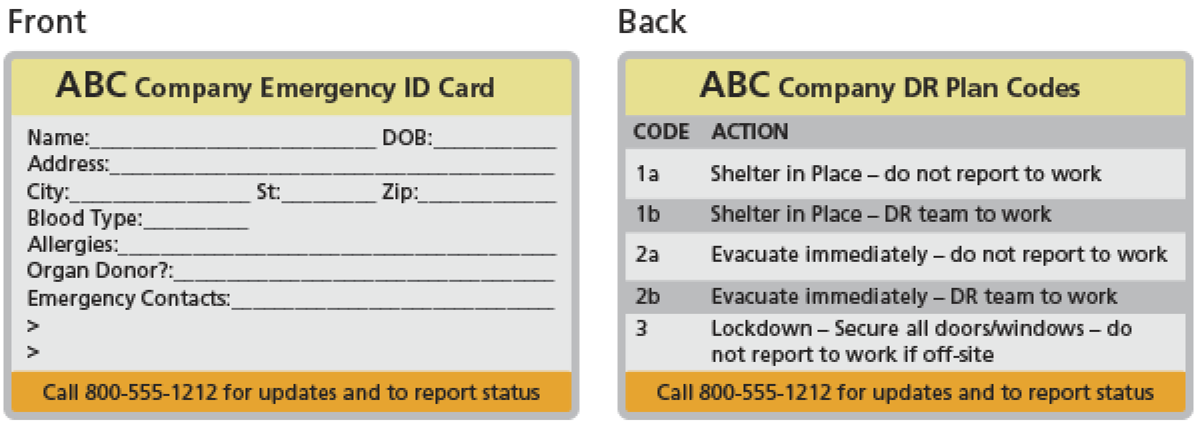
Table 3. NIST SP 800-61, Rev. 2 IR Checklist

		Action	Completed
		Detection and Analysis	
1.		Determine whether an incident has occurred	
	1.1	Analyze the precursors and indicators	
	1.2	Look for correlating information	
	1.3	Perform research (e.g., search engines, knowledge base)	
	1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.		Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.		Report the incident to the appropriate internal personnel and external organizations	
		Containment, Eradication, and Recovery	
4.		Acquire, preserve, secure, and document evidence	
5.		Contain the incident	

6.		Eradicate the incident	
	6.1	Identify and mitigate all vulnerabilities that were exploited	
	6.2	Remove malware, inappropriate materials, and other components	
	6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.		Recover from the incident	
	7.1	Return affected systems to an operationally ready state	
	7.2	Confirm that the affected systems are functioning normally	
	7.3	If necessary, implement additional monitoring to look for future related activity	
		Post-Incident Activity	
8.		Create a follow-up report	
9.		Hold a lessons learned meeting (mandatory for major incidents, optional otherwise). While not explicitly noted in the NIST document, most organizations will document the findings from this activity and use it to update relevant plans, policies, and procedures.	

When the IR plan is no longer able to handle the effective and efficient recovery from the loss caused by an incident, the incident is then escalated to the level of disaster. Disaster recovery planning is the next important component of contingency planning for the Strome College of Business. This plan must have in place the preparation for and recovery from a disaster coming from any type of attack vector—mother nature included. The distinction between an incident and a disaster may prove to be subtle in certain situations. In most cases, a disaster has occurred when either the organization is “unable to contain or control the impact of an incident, or the level of damage or destruction from an incident is so severe that the organization cannot quickly recover from it” (Whitman & Mattord, 2021, p. 208). Such circumstances require a disaster recovery (DR) plan. For example, certain events are immediately classified as disasters, including fires, floods, damaging storms, or earthquakes. One of the key roles of this plan is to lay the groundwork for reestablishing operations after a disaster. But first, there must be a disaster classification to evaluate the amount of damage that could potentially be caused by the disaster. This is to be on a scale of Moderate, Severe, or Critical. Hacker intrusions or malware will fall into the human-made category of disasters, fires or floods will be assigned to the category of natural disasters. There are also slow-onset disasters to be wary of. These build up gradually over time before they can degrade the operations of the organization to withstand their effect (p. 209). These types of disasters can be classified as disasters by natural causes, which include environmental degradation and pest infestation, or they can be classified as man-made disasters, including disgruntled employees and service provider issues. One likely natural disaster for the college to plan for are hurricanes. A likely man-made disaster could result from a social engineering attack via email (phishing). There will also be classification of rapid-onset disasters, which are disasters that occur suddenly with little warning. These include natural disasters such as earthquakes and storm winds, or man-made disasters, including but not limited to distributed denial-of-service attacks or hacktivism. Electrostatic discharge (ESD) is one rapid-onset natural disaster for the college to address in a DR plan. A man-made rapid-onset natural disaster could result from a zero-day exploit. Lastly, as part of the DR plan, certain individuals of the DR team may be responsible for coordinating with local services, such as fire, police, and medical personnel. In addition, during a disaster, the alert roster must be triggered, and key personnel notified of the incident. There must also be a clear establishment of priorities. In this case, the preservation of human life is the first priority, to which data and systems protection is subordinate. Disaster documentation must be carried out as well, which could help to later determine how and why the disaster occurred. The DR plan must also have documented action steps to mitigate the impact of the disaster on the operations of the organization. This may include the evacuation of physical assets or securely shutting down all systems to prevent the loss of data. Furthermore, the plan needs to have in place alternative implementations for the various system components, should primary versions be unavailable. For example, using Dynamic Host Control Protocol (DHCP) to assign network addresses instead of using static addresses can allow for quick and easy connection recovery of information systems without the aid of technical support (p. 210). Finally, as part of DR plan preparedness, each faculty and staff member should always have personal emergency information on their person. This contains information such as who to notify in the event of an emergency, as well as medical conditions, and a form of identification. They should also have on them a set of instructions on what to do during an emergency (an example of an emergency ID card is shown below). This instruction set should contain a contact number for calling the university during an emergency, in addition to emergency service numbers for fire, police, and medical, as well as evacuation and assembly locations, the name and number of the DR coordinator, and any other information deemed necessary.

Figure 3. Emergency ID Card Example (Whitman & Mattord, 2021, p. 210)



Front

ABC Company Emergency ID Card

Name:________________________ DOB:__________
Address:______________________________________
City:______________ St:________ Zip:___________
Blood Type:_________
Allergies:_____________________________________
Organ Donor?:_________________________________
Emergency Contacts:___________________________
>
>

Call 800-555-1212 for updates and to report status

Back

ABC Company DR Plan Codes

CODE	ACTION
1a	Shelter in Place – do not report to work
1b	Shelter in Place – DR team to work
2a	Evacuate immediately – do not report to work
2b	Evacuate immediately – DR team to work
3	Lockdown – Secure all doors/windows – do not report to work if off-site

Call 800-555-1212 for updates and to report status

Disaster recovery plans must be flexible to account for the overwhelming nature of disasters. Once the disaster passes, and the physical facilities are intact, the DR team should begin the restoration of systems and data to work at their fullest potential. If the college’s facilities are destroyed by the disaster, then alternative actions must be taken until new facilities can be acquired (Whitman & Mattord, 2021, p. 211).

Specifications (by Marcos Luchetti)

Core Switches:
4x Cisco Catalyst 3750X-12S-E Switch = $29571.96

Workgroup Switches:
12x CISCO DESIGNED Business CBS350-48T-4G Managed Switch = $6887.52

3x Cisco Business CBS350-8T-E-2G Managed Switch = $810

Routers:
4x CISCO C921-4P = $3395.96

Servers:
1x Cisco UCS® C480 M5 Rack Server = $8749.99
5x Cisco UCS C240 M6 Rack Servers = $14399.95

Firewall Appliance:
1x Cisco Firepower® 1120 = ~$2400

Total: $66215.38

Bibliography

Access control policy and implementation guides. (n.d.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides

Access control policy: What to include. (2021, July 12). Firewall Times. https://firewalltimes.com/access-control-policy/

Botnets: Threats and responses. (2011, April 5). Discover Journals, Books & Case Studies | Emerald Insight. https://www.emerald.com/insight/content/doi/10.1108/17440081111125635/full/html?skipTracking=true

Chapter 7 host hardening. (2017, July 7). SlidePlayer - Upload and Share your PowerPoint presentations. https://slideplayer.com/slide/6894962/

Loyola University Chicago. (n.d.). Loyola University: Loyola University Chicago. https://www.luc.edu/its/aboutits/itspoliciesguidelines/access_control_policy.shtm

National Center for Education Statistics. (1997, March). *Protecting the privacy of student education records*. https://nces.ed.gov/pubs97/web/97859.asp

Network security threats to government and commercial entities. (2020, November 20). https://www.scasecurity.com/network-security-threats-2

Security power tools. (n.d.). O’Reilly Online Learning. https://www.oreilly.com/library/view/security-power-tools/9780596009632/ch14.html

Southern University and A&M College. (2006, November). *Firewall policy*. https://www.subr.edu/assets/subr/NetworkSecurity/Firewall_Policy_and_Form.pdf

Szuba, T. (1998). *Safeguarding your technology: Practical guidelines for electronic education information security*. National Center for Education Statistics. https://nces.ed.gov/pubs98/98297.pdf

What is host hardening and what are some important hardening steps? (n.d.). Yogesh Chauhan. https://yogeshchauhan.com/what-is-host-hardening-and-what-are-some-important-hardening-steps/

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage.