Final Report

Matthew Jacobsen

Connor Greenwald

Group # 10

May 18th, 2021

Executive Summary

As an organization with many moving parts: money flows, personal information storage & retrieval, confidential information, research data, etc… It is highly important to secure these assets to maximize organizational revenue, reputation, and performance. The organization relies on vital mechanisms and systems to process the data and assets including: two databases, two servers, campus internet infrastructure, on campus hardware and workstations, and third party external software packages. All of said systems have vulnerabilities and varying severity if compromised.

There are many threats to these systems which have the potential to cost the organization varying amounts of resources in the form of money, downtime, accessibility, and information. Threats can come from both internal and external bodies, as well as malicious intent and unintentional. Risks posed to the systems include but are not limited to: personal information leakage, misuse of university resources, unauthorized access to university databases, loss of services, loss of data, misconfiguration in hardware / access controls, problematic external software, and social engineering. All of which can have varying effects that could range from FERPA violations, theft of information, system downtime, loss of critical data, destruction or modification of information, and inappropriate use of resources.

In order to provide the organization with proper protection and security there are a set of proposed controls to work in unison to prevent both malicious and unintentional threats to the systems. System backups are automatic and can correct a system failure or loss of data. Personnel education is a preventative measure and will give staff and students the ability to protect themselves and the system from social engineering attacks. Keeping up to date and compatible software, firmware, and information will prevent both malicious attacks on outdated systems, and unintentional compatibility issues. Email filters will process incoming mail to protect users from phishing attacks. Proper incident response, handling, and recording will allow for swift actions upon an attack, and preparation in the future. Finally the anti-malware / Firewall is a standard measure that both prevents, detects, and corrects any suspicious activity the software catches.

To ensure the functionality of the controls proposed for implementation, the organization has devised a number of tests on the controls. These tests show how to gather the data, how to process this data, how to run the tests on this data, and finally it shows objectively what is a passing score vs. a non passing score. Also outlined in this document are the consequences and actions required in the case of a failed test.

Information Security Governance Process

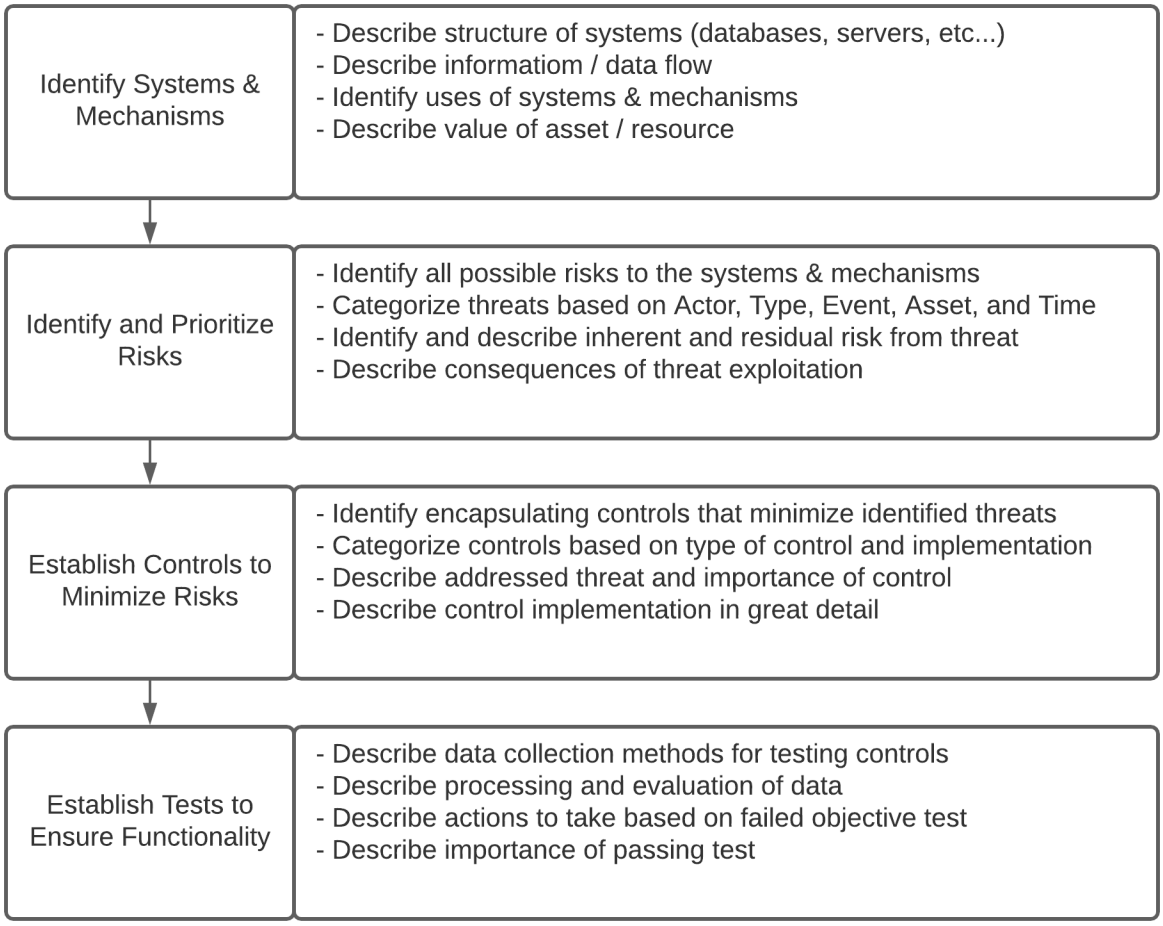

Figure 1: Information Security Governance Process Showing Key Steps in Beaver U's Security

Organizational Description

Organizational Overview

Introduction

Beaver University is an accredited, private, non-profit university located in the heart of the Pacific Northwest. BU offers students a range of over 100 degrees from 7 different colleges. Beaver University is home to nearly 14,000 undergraduate and 2,000 graduate students. The university employs over 300 teaching staff members and another 200 support staff. Along with wanting students to achieve academic excellence, the safety and security of all Beaver University community members is of top priority.

Additionally, BU needs to ensure that all University systems remain fully operational and usable by both students and staff members. The university faces a number of threats, both internal and external, by threat actors who wish to make financial gain from stealing the private data of students and staff members. BU also needs to watch out for any malicious use of university resources which violates University policy. Failure to mitigate these risks could lead to financial losses and a weakening of the University's reputation.

Main Systems Overview

System 1: Databases

Our organization consists of two databases, one where the school's general information is to be held and one that will manage user created data including any student or faculty of the university. Both shall be housed on premise in a secure location with select personnel access. The University's Information Database (UID) generally never deletes data, as it is kept for records. The University Unlimited Storage Database (UUSD) fills with data more quickly and will be deleted 1 year after the student or faculty no longer have affiliation with the university. The UUSD also has downloadable open-source software packages accessible to the student and or faculty (Compilers, Interpreters, Text processors, etc…)

System 2: Servers

The organization will consist of two main servers. One which shall be used for connecting clients to the UUSD either on the University Wifi / LAN / VPN (cannot be accessed from an outside system). This server will allow students and faculty to access university resources, their personal files, and Purchased Software Packages like Microsoft Office. The other Server will be used for the University Website, Student page (grades, classes, address, etc..), 3rd party online learning platform, etc… The server will be run on premises similar to the university databases, and have cloud access on any internet connection. There will also be the university mailing server. This will be the means of communication between all internal emailing, as well as give access to external emails in an appropriate manner.

System 3: Campus Internet / Wifi / VPN

The University will have wired connections to on campus Labs, WiFi, and a VPN for external connections. The on campus internet and Wifi will consist of hardware like routers, access points, wireless adapters, wired connections, ethernet ports, etc… VPN software will be a purchased 3rd party service.

System 4: Computer labs / Student workstations

The university will have on campus computer labs and workstations for students and faculty to take advantage of. These systems will already have wired connections to the university internet and have access to university resources even if the student / faculty are not logged in. These systems will have low level permissions by default. With the default connection to university resources, these may be a target for malicious behavior.

System 5: External Software Packages

The university will also have external software packages. These are both university operational software programs, such as anti-virus software, mailer spam detection. Also included are purchased software packages from MS and Adobe such as Word, Powerpoint, Photoshop, etc... These assets are provided by the company and also implemented (low liability). Resources for students / faculty can be accessed via their university login on the resource website and downloaded.

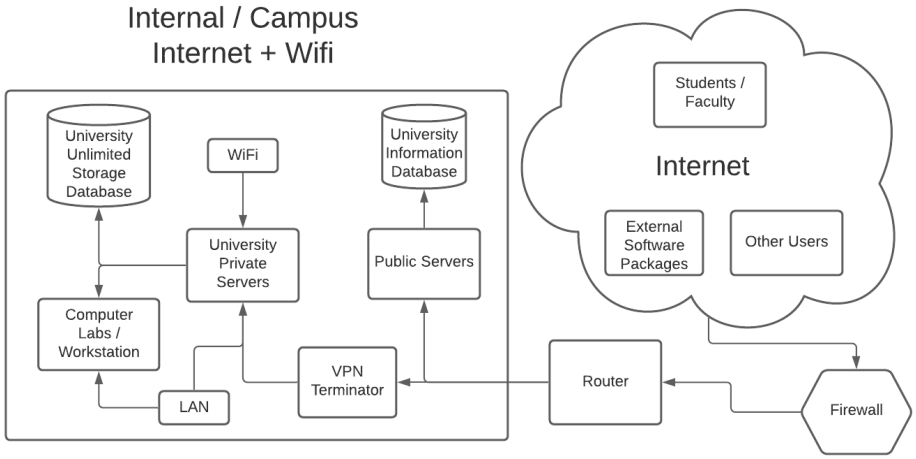

Figure 2: Diagram showing the organization of Beaver University's IT systems

Risk Assessment

Risk Assessment Philosophy

Beaver University will take a bottom up approach to evaluate the risks associated with operating a higher education institution. We believe a bottom up approach to be best suited for our needs because an institution such as ours is not unique-- meaning knowledge of the risks and vulnerabilities that other universities are exposed to can be used to help us assess the risks we may face. We will use common vulnerabilities and assess their relevance to our organization and enact measures to mitigate any vulnerabilities which we believe puts our organization at risk. Below are a number of vulnerabilities and their risks that our university could encounter.

Risk	Actor	Threat Type	Event	Asset/Resource	Time
Personal Information Leakage	Internal External	Malicious Unintentional	Improper Disclosure FERPA Violation Theft of Information	Private or FERPA protected personal information	Anytime Instantaneous
Misuse of University Resources	Internal External	Malicious Unintentional	Interruption or slowing of services Illegal use of resources	Computing power	Varies
Unauthorized Access to University Database	Internal External	Malicious Unintentional	Improper disclosure Theft of data Modification of data Interruption to services	Private/financial data Intellectual property	Continuous access until noticed and prevented
Loss of Services	Internal External Nature	Malicious Unintentional External services Acts of god	Interruption to services Inappropriate use	University hosted software servers, website	Several hours to days
Loss of Data	Internal External Nature	Malicious Unintentional External services Acts of god	Interruption to services Loss of data Modification of data	Data Backups User Information General Data	Time to restore from backup (if available)
Misconfiguration in Hardware / Access Controls	Internal Nature	Malicious Unintentional	Modification of data Loss of data Theft Destruction	User Data IT Infrastructure Information and Application Process	Several Hours
Problematic External Software	Internal External	Malicious Unintentional	Interruption Disclosure Theft Destruction	User Data Information and Application Process	Based on an external company. Likely several hours.
Social Engineering	External	Malicious	Improper Disclosure Unauthorized Access	User/ Financial Data Private information	Minutes

Inherent and Residual Risk

Misuse of University Resources

Anytime an organization provides resources, whatever they may be, to members of the community there comes the risk for potential misuse of those resources either by breaking policy or real world laws. There are many cases of misuse of university resources that BeaverU needs to watch out for. Giving students and staff access to computing power and storage may lead to some individuals using the resources for illegal activity such as downloading and hosting pirated content. In more extreme cases, Beaver University processing power could be used for malicious actions like participating in a botnet to perform DDOS attacks. While not illegal, some users may break university policy by using shared computing power for personal benefit such as by mining crypto currency, hosting personal websites, or storing non academic data.

Automated monitoring would be put in place to prevent the misuse of university resources, however determined individuals may be able to bypass security measures. The measures put in place are not meant to stop 100% of misuse, just the vast majority while also alerting to any other misuse that is detected. The university may still be at risk for users hosting personal or pirated content if users can bypass the automated detection systems put in place. Finally, advanced malicious actors may be able to bypass security measures to use university computing power for a short period before the activity is noticed and prevented. While these measures cannot prevent all risk, the residual risk is greatly reduced.

Loss of Data

Loss of data can have costly consequences for the university depending on what systems are affected. The most costly of which would be if the databases holding Beaver University's financial records become corrupted or inaccessible for whatever reason. In this event the university could potentially lose payroll records, student billing information, and department budgets. The university also creates and stores a large amount of non-financial data that could potentially be lost. This data includes: faculty and student research, teaching material, intellectual property, website data, academic records, and any other data that is being stored on university equipment.

To help mitigate any potential losses, Beaver University keeps daily backups stored at an offsite location. While this helps prevent the loss of important data in most cases, some residual risk remains which is infeasible to reduce further. There is the small, but possible likelihood that both the original data and the backups could be destroyed in the event of something like an earthquake that affects both the university and the offsite storage servers. In the event the data backups are required data may not be permanently lost, however, the time to transfer the many terabytes of data from offsite to the university may leave many critical services in operable for an extended period of time.

Misconfiguration in Hardware / Access Controls

Misconfigured access controls and hardware can be catastrophic without the proper measures taken to prevent these. There are a number of ways someone could perform both malicious and unintentional actions that would be damaging to the organization. These could range from a student using an administrative computer and changing their grades, deleting data, or even creating a backdoor for future use. The inherent risk from poorly configured hardware and access controls could cause anything and everything to occur to the data, information, resources, contacts, people, and money. These issues may be specifically important to defend against on campus, but it is also possible for a remote machine to have too many permissions and perform malicious actions that can have catastrophic repercussions.

It is very simple however to implement access controls on both on-campus devices, machines, and systems, as well as remote devices and connections. Therefore after the implementation of access controls and correctly configuring hardware there should be few residual risks. These could be from a phishing attack to get admin access, or an internal actor that has malicious intent to give more permissions than are meant to be to other people. There is always the risk of a hack that bypasses these permissions as well. When the correct configurations and permissions are implemented the organization will only be left with intentional malicious residual risks that can range in outcome and severity. Generally speaking, bypassing access controls grants an attacker access to modify, delete, and steal data. They could also modify systems and permissions.

Control Structure

Control Framework

Beaver University will primarily be using CIS[1] Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs). As a medium sized university, Beaver U does not have a vast budget to fund cyber security operations which made this framework a good starting point as it is cost effective. This guide closely aligns with our organization's resources, systems, and information necessary to protect our organization. This framework will guide the organization to implement the necessary controls to have a strong base of security through cost effective education, system controls, 3rd party monitoring, encryption, and configuration to protect us against the key risks which have been identified under the 'risk assessment' section. Where necessary, the organization will also refer to the NIST[2] guidelines and standards for more extensive security in areas where our organization is outside the small-medium scope, such as data management, email server security, etc. For the more complex systems, NIST's Risk Management Framework[3] will provide controls and implementation measures such as system backup's, media storage, and wireless/remote access.

Control Name	**Type of Control**	**Implementation**
System Backups	Corrective	Automatic
Personnel education	Preventative	Manual
Authorization / Dual Authorization / Access Controls	Preventative	Hybrid (permissions are managed, and can be overridden)
Software, Firmware, and Information Integrity	Preventative	Hybrid (Automatic updates, manual actions on software no longer supported)
Malicious Email Filtering	Preventative	Automatic
Incident Response / Handling / Recording	Preventive / Corrective / Detective	Hybrid
Anti-Malware / Firewall	Preventive / Detective / Corrective	Automatic

[1] *Center for Internet Security.* *https://www.cisecurity.org/*
[2] *NIST: National Institute of Standards and Technology.* *https://www.nist.gov/*
[3] *NIST Risk Management Framework.*
https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53

Control Narratives

System Backups

System backups are in place to control the risk of **Data Loss.** The organization adapts this control from NIST CP-10[4] System Recovery and Reconstitution. Data loss would bring major loss of revenue to the university depending on which data is lost, if not all. Billing information would be costly, as these records are needed to know who owes the university what amount of money. Other data could be research data which would be very costly as the data would need to be gathered again or the research project would need to be dropped completely.

A data backup is relatively simple but effective and specialized. The implementation would work as follows: The university would hire a third party data center to manage the backups of all university data deemed necessary, which likely would be all of it. Financial records and other top priority information would be backed up to the data center every 10 minutes for extra safe measure. Information less important such as student file data would be backed up every 30 minutes to the other data center.

This control falls under **corrective.** This is because the backup of the data is in no way preventing data from being lost or corrupted from our main data facilities, however when this data is lost or corrupted the backup then corrects this mistake by transferring the latest backup to the main data site to restore the previous state of data.

This control is an **automatic** control because it does not require any human attention to backup the files to the backup data center. When the control is configured there may be a few things that can manually be done, like manually transferring the backup to the main, but overall the idle of the control is purely automatic.

The control will be tested for functionality by an automatic tool that checks once a day to see that the backup is nearly up to date with the main data center. The tool cannot compare both data cites thoroughly at the same time so it will pick random aspects to be sure that data is not corrupt and that the data is caught up to the main data center.

Personnel Education

The security of an organization can only be as strong as the weakest link. Unfortunately, in most organizations it is the employees which are most susceptible to a variety of social engineering attacks. Social engineering is an attack aimed to bypass control measures by tricking a human into performing an action or allowing an attacker to perform an action that compromises the security of the organization.

Beaver University recognizes that social engineering is a serious threat that has the potential to cause severe damages to university assets and resources. To help mitigate the risk of **social engineering** Beaver University will implement several controls which all relate to **personal education and employee training** so that employees can better spot and prevent social engineering attacks. The primary control measure put in place will consist of twice-yearly training workshops. These training sessions will be led by an organization that specializes in

cybersecurity training and follows the NIST Awareness Training & Education Standards[5] which have been contracted by the university. Not only will employees be taught about types of attacks, but also what the proper protocol is if they were to identify an attempted social engineering attack and the proper actions they should take if they realize they have fallen for social engineering.

The control of education for all university wide employees is a **preventive** measure. The goal is to enable employees to have the skills necessary to identify and respond to social engineering attacks before one takes place. While there will be corrective and detective controls put into place to detect and respond in the event an employee falls for a social engineering attack, but ideally the preventive measure of training all employees will lead to a reduction in successful social engineering attacks.

Implementing twice-yearly workshops will fall under the category of a **manual** control. Training sessions will be a time consuming and expensive process, but Beaver University believes that the cost will be well worth having well informed employees.

To gauge the success of the control measures put into place, Beaver University will implement various tests to make sure employees understand and are following the social engineering safety best practices. Initially, at the conclusion of the workshops all employees must take a written questionnaire that reviews the concepts they have just been taught. All employees will be required to answer all questions correctly. Employees with incorrect responses will be asked to review the learning material and correct their answers. At random times throughout the year phishing test emails will be sent to employees. These emails will look very similar to what a real phishing email looks like. Any employee which clicks on a link found within one of the test phishing emails will be documented and the employee will need to take a refresher course on how to stay safe from social engineering. Finally, from time to time the university will hire penetration testers to perform various social engineering attacks. The reports generated following the penetration test will be used to evaluate how university staff responds to social engineering attacks and the effectiveness of the training. Future training sessions will be tailored based on these metrics.

Authorization / Dual Authorization / Access Controls

Correct authorization and **authentication** of users on the system is of utmost importance because the risks associated with authentication are high. This control is largely taken form the NIST Access Control Family[6], namely AC-1[7], AC-2[8], AC-3[9], AC-17[10], and AC-18[11]. These combine for a control on overall access controls, as well as wireless and remote access controls. Every identified risk the organization has is related in some form to this control. It is very important the organization implements these controls correctly to avoid a malicious user that has more permissions than intended.

In order to implement this control the organization will be outsourcing to a third party for dual authentication such as DUO[12]. This way a corrupt password to an account does not allow a malicious user to access their account. The organization will also implement least privilege across all aspects of the university. From on campus hardware to VPN users. The system will only allow the user to use the least amount of resources and permissions required to complete their job.

This type of control is **preventative** because all the control is doing is preventing a bad actor from getting permissions that could be damaging to the university. It is not corrective as once the deed is done the access controls won't have any effect. It is also not detective as the access controls don't know when someone has more access than they are allowed. There is one aspect of detective though and that is with our third party provider of dual authentication, when someone attempts to login to an account with the correct credentials the user will be notified. This gives knowledge to the user about a corrupt password and requires further attention.

The implementation of this is mainly **automatic** once setup and running, however many times there will be permissions and access controls that need to be overridden in special cases. These cases can range from students losing their phones for dual authentication, or a public computer that needs updating and is given administrative permissions to run updates, etc...

The organization will track the functionality of this control by having a review on permissions at the end of each term that is done automatically, with some random manual checking. There will be an up to date list on university devices and their granted permissions that will be manually checked once a term. DUO authentication will also be required to notify students and the university of a failed login attempt which signifies the student or faculty did not attempt to login but someone else did with correct credentials.

Anti-Malware / Firewall

Beaver University is a potential target which some adversaries may wish to harm. To address the risks of **misconfiguration of hardware / access controls, loss of data, and unauthorized access to university resources** Beaver University will install **anti-malware** software on systems and create **strict firewall rules** which restricts unwanted internet traffic from reaching the university. Malware prevention software will be chosen and configured according to NIST 800-83[13] standards to ensure proper prevention and response to any malware related incidents. Similarly, the Network firewall rules will be written following the guidelines from NIST 800-41[14].

These controls will consist of a combination of **preventive, detective, and corrective** measures**.** Anti-malware software and the firewall will be used initially to prevent any files or network traffic that has been flagged as suspicious from interacting with the university network or systems. The anti-malware software will also run regular scans of file systems to detect any files which contain the common signs that may indicate malicious software. In the event that malicious software is detected, the software will take corrective actions by quarantining the software from the rest of the system until the software has been manually reviewed and determined to be safe or malicious.

These controls will be an **automatic** approach. Initially, the software and firewall rules will need to be manually configured by IT staff following the NIST guidelines mentioned above. However, after the initial setup the anti-malware software and firewall will be able to work autonomously. In some events, human interaction may be required to determine if software or network traffic has been improperly flagged as suspicious, but for the vast majority of the time this control will act in an automatic fashion.

To gauge the success of the controls, extensive logging will be used when the firewall or malware software marks activity as suspicious. Additionally, when human interaction takes place it will be documented. At regular intervals, IT staff will evaluate the percentage of false positive malicious flags and false negatives which manage to bypass the anti-malware and firewall. This data will be used to adjust the software to become stricter or more lax depending on what the data indicates.

Software, Firmware, and Information Integrity:

Keeping our software, firmware, and information up to date and supported is crucial to not only provide functioning resources to the faculty and students, but it is also incredibly important for security measures. The organization has adapted this control from NIST SI-7[15] with a larger focus on updating and maintaining software, firmware, and hardware. This control is closely related to **loss of services**, and p**roblematic external software.** Loss of service is somewhat acceptable and can be dealt with in a timely manner, however the university cannot afford to not patch an operating system, or software, that results in an exploited bug.

This control will be implemented by having by default all machines on automatic updates that update overnight when not in use, or less use. 3rd party external software packages will be updated on the university's devices, but when on a student's machine the university cannot force an update. All hardware, firmware, and software will be routinely checked for compatibility by using a running list of university resources. As soon as a manufacturer or company rules a certain product no longer secure with today's technology the university will replace the product with an updated version.
This control is a **preventative** measure because it is preventing the exploitation of out of date software and hardware. By keeping all products up to date on the organization systems the organization is ensuring that the most recent bug patches have been patched because likely the first place a malicious user is going to attack bugs is big systems that run outdated software.

The implementation of this control falls under a **hybrid** approach. While all the software will be on automatic updates and won't need anyones attention, there may be software that no longer gets updated or patched, and at that point it will require intervention to find an alternative software that can be supported and secure with current systems. Also, hardware and firmware may no longer be supported and may need replacing and updating to ensure compatibility and security.

The organization can measure the success and functionality of this control by hiring penetration testers to attempt to hack into the systems the university is using. Another method would be to provide a bounty for any software, firmware, or hardware found that is no longer secure or compatible with the system so that after the controls have been implemented there is an incentive to find any software that is exploitable.

Malicious Email Filtering

Malicious email filtering relates to the **social engineering** risk and is adapted from NIST SI-8[16] Spam Filtering. This control is in place to filter out incoming emails towards users in the system that are likely to be phishing or otherwise malicious emails. This way on top of the education towards the organization's faculty and students, there is another wall of protection that emails must first pass through.

The implementation of this control is going to be a third party email filter that is up to date on common and trending email attacks. Also, any suspicious emails that don't pass the highest threshold will be given a warning when delivered to the user so that they are reminded this is possibly a malicious email. The university does not have the resources to implement their own software filter so it is much more cost effective to outsource this to be the most efficient and effective possible with a program that is up to speed on all modern attack mediums.

This control is purely **preventative**. This is because all the email filter is doing is preventing certain malicious emails from ever reaching the user to rule out the most obvious and outstanding phishing attacks.

The implementation of this control is **automatic** because it requires no personal attention and will be running on the cloud, and updated and maintained by the third party provider. The only human intervention is minimal and may come about if an email gets through that is reported as a phishing email.

The organization will be able to measure the effectiveness of this control by sending in their own phishing and malicious emails to test the software. Any emails that make it through that are malicious should be flagged as a warning for the user and if they are not the third party provider will be contacted for further assessment of the effectiveness.

Incident Response / Handling / Recording

This control is an all encompassing control that covers **all risks** because it has to do with any issue the organization encounters that needs proper handling and an IT team and executives to decide course of action and proper records. This control is adapted from the NIST Incident Response Family[17]. The adaptation is largely generalized to the family and does not entail specific controls from NIST. Without the proper incident response an attack or other exploit can last longer and be more damaging. Also, once an event has occurred it is important to record and learn from the event in order to prepare for the future.

This control will consist of a team, a hierarchy of events, a plan of action for events, and standards for records. The team will be composed of IT professionals and executives at the university. The IT team is responsible for action on the event, and the executives are responsible for best action for the organization as a whole. A hierarchy of events tells the team what to do in certain scenarios depending on the severity of the attack. Plan of action for certain events tells the team what to do, who to contact, and measures to take in the case of a specific event. Finally a standard for records lays out how the team should handle and record the events to hold for legal purposes as well as future implementation of controls.

This control is **preventative, corrective, and detective**. The control is generally all encompassing as a dete method, to lead to a course of action in order to professionally respond to an event, as well as prevent future events.

The implementation of this control is **hybrid**. SOC tools will be used to automatically collect and store all network data traffic. Automatic systems will scan this data looking to identify any known indicators of compromise (IoCs) which will be sourced from external services. When IoCs are detected security analysts will be notified and they will take any manual corrective actions required to resolve any issues which may arise.

The organization can measure the effectiveness of this control by having practice incidents to monitor the response, handling, and recording of certain events. From there a third party can analyze the team's response and performance to better understand and improve on techniques and on paper action.

Control Tests

Employee Training - Manual

As previously described, a series of metrics will be reviewed quarterly and used to determine the effectiveness of the personal education and social engineering awareness training:

- A written questionnaire reviewing the content of the training workshop
- Test phishing emails
- Penetration tests

Questionnaire

Written questionnaires that have been accurately completed immediately following the training sessions will be collected and serve as proof that employees have completed the required training. In order to pass the questionnaire employees must correctly answer every question. Employees with incorrect solutions will be asked to review the material and attempt the incorrect questions again. Failure for an employee to attend a training session or fail to answer all questions correctly would indicate a lack of social engineering awareness and could expose Beaver University to moderate to severe risk if an employee were to fall for a malicious social engineering attack. To combat this, training will be modified to address topics which employees commonly have issues with.

Phishing Tests

Phishing tests will be conducted at random intervals throughout the year and performed by a contracted cybersecurity firm. Specifically, emails that appear to be legitimate but are actually phishing emails will be sent to a sample of employees. Clicking on any link contained in the phishing email would constitute a failure. Employees will be expected to report these phishing emails to Beaver University's security, but will not be required in order to pass the test. Even a single employee failing the phishing test could expose Beaver University to severe risk via account compromisation. In the event of a greater than 1% failure rate for a phishing test, additional training will be provided for all employees.

Penetration Testing

Penetration test will be performed regularly, testing both the organizations online infrastructure as well as the physical access controls. Penetration tests will be performed by an external penetration testing company and an official penetration test report will be used as a metric to determine the success of the current controls. All security concerns disclosed in the report would be addressed, but a passing penetration test would be considered one that discovers less than 3 minor security issues with no intermediate, severe, or critical vulnerabilities. A report disclosing greater than 3 minor vulnerabilities/information leaks or any number of more serious vulnerabilities will be considered a failure and new controls will immediately be introduced. A penetration test failure would directly expose the university to whatever risk has been discovered. Failure to resolve a disclosed risk would not only expose the university to the

vulnerability itself, but could also lead to the university being found negligent for failing to correct a vulnerability it was aware of.

Malicious Email Filtering - Automatic

Penetration Testing

The first measure to test our Malicious Email Filtering control would be to attempt to get past the filter by using a hired penetration tester. This group / individual would be a third party hire that has experience getting past various email filters.

The data our organization would be looking for is a ratio of emails that were caught and not allowed through, to emails that were allowed through but with a warning flag, and emails that were allowed through with no warning flag.

The acceptable range would be the following:

- = 0% of malicious emails allowed through with no warning flags
- < 5% of malicious emails allowed through with warning flags
- > 95% of malicious emails not allowed through at all

If any of these criteria are not being met, the organization will need to re-evaluate the effectiveness of the control and decide if either the criteria are possibly unrealistic, or the organization should begin searching for a more reliable contractor to hire for the maintenance of the email filter. Although the organization has other controls in place to stop social engineering attacks via email, if the criteria are not met it poses a higher risk to the organization than the organization is willing to accept. This would mean that there are more opportunities for an attacker to gain access to accounts, data, and systems that could be catastrophic to the organization. It is vital that the organization keeps these criteria met such that preventing opportunity for successful attacks.

Emails Caught vs. Reported

The second measure to test the success and functionality of the organizations Malicious Email Filtering Control would be a similar method to the penetration testing, but instead of relying on a third party contractor to test the system this would rely on the raw data and reports from the users of the emailer from students and faculty.

The data would come from two places. The first would be the total number of emails not allowed through from outside sources which would come from the third party email filter. The second source of data would be from users of the emailer, students and faculty, who report any emails that are deemed suspicious or possibly phishing.

Considering not every malicious email allowed through is going to be reported, this criteria is less precise. The organization will deem the following criteria acceptable for this measure of the control:

- For every 250 emails not allowed through 1 or less emails must be reported

With this measure the organization can be confident that very few obvious malicious and phishing emails are allowed through to the users. This way they are protected from outside attacks with malicious intent. If the organization detects many more emails reported than allowed, a re-assessment must be conducted to either re-calculate the criteria, or search for a

better email filter.

Random Quarantined Email Sampling

The last measure to confirm our email filter is functioning properly is to randomly sample the emails not allowed through to ensure they are indeed malicious emails and not being quarantined when they shouldn't be.

The data will be taken from a manual approach by sampling 100 emails per week with the help of an employee of the IT department with a background in cybersecurity. The allowable criteria is as follows:

- 0 emails mistakenly quarantined

If the criteria is not met, there will be a case by case examination as to why the algorithm did not allow the email through, and the organization will ask the third party email filter to re-examine similar emails and confirm that no more similar emails were mistakenly quarantined. If the committee rules that there are too many emails being handled improperly the organization will ask the third party to loosen their standards, which in turn affects the other measures of success. A re-evaluation would need to take place if such events occur.

It is important that this criteria is met so that our users are getting the emails that are meant to be delivered to them. These could be important job opportunities, account information, bills, etc… Our users are not encouraged to use their email for anything other than academic purposes, but in the event they do register a third party account or subscription under their university email the user should still be receiving important emails.

Policy Recommendations

Beaver University's primary goal is providing students with a higher educational opportunity while keeping all members of the University's community safe from all threats internal and external. This goal can not be satisfied unless there are set procedures in place which clearly define the steps to report incidents when they may occur.

Malicious phishing emails represent one of the most common attack vectors which our university faces. A compromised account can give an attacker the foothold they need to allow them to pivot into more serious attacks. These attacks could harm Beaver University's financial bottom line, private user data, or its reputation as a college. Even with these known potential risks, employees are often apprehensive to report that they have fallen for a phishing email due to fear of punitive consequences. The combination of phishing being a common attack, having severe consequences, and employees being hesitant to report leaves our organization at severe risk. As a result, we find it important to recommend clearly defining a set of procedures which students and employees are expected to follow if they believe that they have been compromised as a result of a phishing attack.

The 'phishing email incident response procedure' will contain two parts. The first is for the account holder and the second is for the security team. In the account holder section, the procedure will first cover the key ways which owners can identify if they have fallen victim to a phishing attack. The produure will first instruct the account holder to look for signs that the email is illegitimate. This may include links which contain unfamiliar URLs, multiple spelling and grammar mistakes, emails containing time sensitive calls to action, and emails which come from outside of the university. The procedure will also inform account holders how they can identify if they have been compromised by viewing their last login time and by identifying account activity which they do not recognize. In the event that an account holder believes their account has been compromised or that they have fallen for a phishing email, the procedure will instruct the user to immediately change their password and report the incident to the security team. The procure will make note that reporting a phishing incident may require extra training, but failure to report the incident could lead to more serious consequences.

In the security team section, the security member will be first instructed to lock the compromised person's account and reset the password. The security team member will then review the compromised account's recent activity and rectify any issues they encounter. This could include removing malware, sending warnings to students and staff that they have been sent content by a malicious user, or take any other action to prevent further security incidents. When the account activity has been reviewed and once again deemed safe, the account can be unlocked and the account owner can once again reset their password to regain access.

References & Appendix

1. https://www.cisecurity.org/
2. https://www.nist.gov/
3. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53
4. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=CP-10
5. https://csrc.nist.gov/Projects/Awareness-Training-Education
6. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=AC
7. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control/?version=5.1&number=AC-1
8. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control/?version=5.1&number=AC-2
9. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control/?version=5.1&number=AC-3
10. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control/?version=5.1&number=AC-17
11. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control/?version=5.1&number=AC-18
12. https://duo.com
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
14. https://www.nist.gov/publications/guidelines-firewalls-and-firewall-policy
15. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=SI-7
16. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=SI-8
17. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=IR