Operation Manual

Final Draft

Brandon Cano

ECE:5840 - Software Security
5/9/24

Contents

Chapter 1

Introduction

1.1 Document Intentions

This manual serves as the comprehensive guide detailing operational procedures and work flows within our company, ensuring a safe, secure, and efficient standards across all our company's activities. This manual is designed to be our company's internal policy, providing clear requirements for all employees regarding their roles in maintaining security measures.

Security within our company extends beyond our technical personnel. This is meant to encompass every member, including janitorial staff, administrative personnel, software developers, etc. Each security policy outlined in this manual will state its relevance to different roles within the company. Along with that, items will be explained in many different ways to encompass the ease of use when reading some of the more technical aspects of the manual for those who may not be familiar with them.

1.2 Document Overview

This manual is structured to provide a detailed understanding and outline of various aspects critical to our company's operations. It encompasses policies and procedures related to:

- Confidential document sharing within the company
- Implementation and management of an externally purchase storefront
- Evaluation and deployment of the storefront

1.3 Intended Audience

The primary audience for this operation manual includes members of the board of directors, who are tasked with overseeing and approving the policies outlined in this manual. Additionally, all employees of this company will be addressed within this manual for any security measures that may directly apply to them.

Chapter 2

Access Control

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Access control is a fundamental concept and one of the most central and important concept in computer security. This is because access control determines who can access what resources and how. It is important for the following reasons:

- It protects the confidentiality, integrity, and availability of data from unauthorized users and malicious attacks.
- It enables the enforcement of security policies and regulations, such as the principle of least privilege and separation of duties.
- It facilitates the management of users, groups, roles, permissions, and credentials, enhancing authentication and authorization efficiency.

2.1 Access Levels

An important part to create a secure systems of control has to do with the access levels of the users within the company. To achieve this, all protocols will be based on a concept of a "need-only" basis when it comes down to permissions. This means that the different activities and permissions that an employee has access to are granted solely based on the job requirements of the individuals. The reason for this is that if everyone has access to confidential resources then it will not be as difficult for an attacker to find a weak link and be able to gain that access as well. Whereas, if only the personnel who need it for their job have this access then it can greatly reduce some of the risk in that area. This approach ensures that employees are granted access only to the activities and resources essential for their roles, minimizing the risk of unauthorized access to confidential data and resources.

2.1.1 Role-Based Access Control

Our main system of access control that will be utilized is role-based access control (RBAC). The way this works is that people are given different permissions and access rights to various resources and data based on the roles that are created within our company. This allows for the efficient management of user permissions by associating them with specific roles. Each role is defined based on job responsibilities and access requirements, meaning with proper management

of users and their roles, employees should only have access to what they need to do their job without access to things they do not need.

The reason for using this system is because it has a few benefits that will work well with our company.

- Simplicity: Managing user permissions by grouping them based on common job requirements and functions.
- Scalable: As the company grows, RBAC makes it easy to add new roles and allow adjustments of permissions to accommodate changing business needs.
- Security: By granting access on a "need-only" basis, RBAC minimizes the risk of unauthorized access and data breaches.
- Accountability: If a certain action is performed that is seen as a risk, RBAC makes it easy to find a traceable link between each role and users that have them.

Everyone in the company will have roles assigned to them no matter what their job is within the company. Even those who do not have a company device, they will have a role they does not give them any permissions, though they might require physical access to different areas of the buildings. That, however, will be discussed in a later chapter.

2.1.2 Implementation

In order to properly get the RBAC system up and operational there are some steps that need to take place in order to accomplish this.

1. Identify Roles
2. Define Hierarchies
3. Map Permissions to Roles
4. Assign Users to Roles
5. Monitor Role Changes

To start, begin by identifying distinct roles within our company based on all the different job responsibilities and our data/resource access requirements. Roles should be small enough to accurately reflect the various access needs of users across different departments and jobs. For example, there may be different engineer roles depending on the different departments they may be apart of.

Next we want to define any role hierarchies that may be present for the different teams or departments. This will help determine role inheritance where it may be utilized. This inheritance can be used to give people with more responsibilities more permissions based on the permissions of individual in "lower" roles have access to. For example, an engineer may only only have permissions to modify files within a project. Whereas the production engineer, who inherits the properties of the engineer role, may also have the ability to manage the production code base and publish changes to that.

Now to map permissions to their roles, we need to know what items must be accessed for someone to do their job. For example, individuals who work on the storefront will have vastly different permissions than those who have to handle confidential internal document sharing.

Once all the permissions and roles are defined, we can check who is in which department and add the various roles to all the users who qualify for them.

As operations take place roles may need to be updated or modified, in case this happens there must be a monitoring system to know when and by who the changes occur. This is allows us to be able to identify any potential security risk if an unauthorized change occurs.

2.2 User Permissions

When it comes down to the user permissions, its important to be able to monitor the ”what and why” for everyone within the company. By enforcing reviews and resets of permissions, we can lower the risk of potential security threats from any outdated or unused permissions someone may have. To help keep a system in place with a way to enforce these changes a few different protocols and strategies will be used.

- Annual permissions reset
- Permission approval process
- Automation with monitoring

As part of the access control protocol, user permissions are reset once a year. This is done to ensure we remove any unnecessary roles any individuals may still have and no longer need. On top of this, the user will then need to put in a request for their roles that they will need to resume their work, which they will then be approved or denied. This protocol helps prevent user from collecting unneeded permissions over time, reducing the risk of unauthorized access.

After a yearly reset occurs, in order to regain permissions, employees must request approval from their respective managers. In this request they must provide all the roles they need as well as the business case for them. The managers must be aware of the current roles and duties of each member of their team to ensure they are getting what they need. If the roles that are needed ever change throughout the year due to changes of business needs, they are expected to make note of these changes.

To make sure the roles are reset there will be some automated process to facilitate the reset process and monitor changes that occur. This system will include all the timestamps when someone lost all permissions, when a request form was submitted, the contents of the form, and what items were approved and denied, if any.

Chapter 3

Awareness and Training

(i) *Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulations, and policies related to the security of organizational information systems; and*

(ii) *ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*

This section outlines the importance of cultivating a culture of security consciousness within the organization. Through training courses we can aim to ensure that managers and users are all well informed of the security risks associated with their jobs. By investing in the awareness and training of our personnel, we help improve our organization against potential weaknesses that unaware users might impose.

3.1 Management and Organizational Information Systems

For all of the training that everyone is required to do, its imperative that the management personnel encourage and enforce everyone to gets their training done in a timely manner. This is because managers play a pivotal role in setting an example for their teams by encouraging and overseeing the actions that are occurring. One way this can happen is by regular communication, briefings, or updates on any emerging threats and security protocols ensure that everyone is being vigilant.

3.2 Personnel Training

For all personnel within the company, they will have to complete a set of training courses and videos that outline and highlight the risks that their jobs could impose on the company. For each different types of risks, threats, or attacks that they can encounter they will need to complete the training courses soon after a new hire is added to the company. On top of that at the beginning of each year every user will have to redo each course associated with them to help refresh the memories of all personnel. This can allow opportunities to include or refresh different videos and courses to help keep the information relevant to the ever-evolving landscape.

Chapter 4

Audit and Accountability

(i) *Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and*

(ii) *ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.*

In our systems and servers, every confidential action or special permission must be recorded to ensure comprehensive auditing, analysis, investigation, and reporting of unlawful or unauthorized use of confidential data and system activity. This is critical for maintaining the security of our confidential documents, enabling us to detect and respond promptly to any potential security breaches. By adhering to audit and accountability practices, we can trace the actions of individual users to hold them accountable for their actions and prevent malicious activities that could compromise the confidentiality, integrity, and availability of our systems.

4.1 Auditing

For every action that requires special permissions, such as accessing confidential documents or performing administrative tasks, it is crucial that these actions are recorded in audit logs. The audit logs serve as a record of all system activities, allowing us to monitor and analyze user actions for any signs of unauthorized or suspicious behavior. In the event of a security breach or incident, these audit logs play a huge role in identifying the source of the attack. This enables us to determine the initial cause of the incident and take appropriate recovery and prevention measures. Our auditing policies ensure that no activity goes unnoticed, providing us with the information needed to maintain a secure environment. The items that should be tracked are as follows:

- Accessing and sharing confidential documents
- Emails with any confidential labels
- Any changes to the store front
- Key card access to rooms
- Downloading of software found online

By recording access to confidential documents and resources helps us track who has viewed or modified sensitive information. This is crucial for identifying potential unauthorized access or leaks of confidential data.

Monitoring emails with confidential labels ensures that sensitive information is not being improperly shared outside the organization. Prior to the email being sent out the automated system will scan the contents and identify any sensitive information and then prevent the email from sending if the proper labels are not being used. This is especially used when sending emails externally since we do not want to have any accidental disclosures of confidential data.

Changes to the store front, such as updates to the website, may impact the security and integrity of our company's systems or premises. Likely these changes are recorded through Git if code is being modified by out software engineers.

Access to restricted areas like server rooms should be closely monitored to prevent unauthorized entry and potential data breaches. Audit logs can show us who key carded into certain areas and when, aiding in any investigations of security incidents or breaches.

Downloading software or files from online websites can easily introduce security risks such as malware, worms, viruses, or any other unauthorized software that may compromise system integrity or expose sensitive data. We can generally prevent people from doing this but in the cases where individuals need this, we can log these actions to help in identifying potential security threats and enforcing policies regarding software usage and downloads.

4.2 Accountability

Accountability is fundamental for enforcing our security protocols, ensuring that individuals are held responsible for their actions. With our Role Based Access Control (RBAC) mechanisms, we can uniquely trace the actions of individual users to their accounts, roles, and the company's audit logs. This enables us to identify and address any malicious activities quickly and confidently. In cases where individuals misuse their access privileges or engage in prohibited actions, either by accident or intentionally, accountability measures are implemented to enforce disciplinary actions and deter future misconduct. Some disciplinary actions that can be enforced are:

- Warning
- Account lockout
- Permission or role removal
- Department relocation
- Termination

It should be noted that these are the most common actions and each one will depend on the severity of the violation and the context behind it. Management and system administrators will have to make their best judgment when choosing the proper disciplinary actions. Though, by maintaining our protocols of accountability, we can then keep the integrity of our systems, further protecting our company from both internal and external threats.

Chapter 5

Certification, Accreditation, and Security Assessments

(i) *Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;*

(ii) *develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;*

(iii) *authorize the operation of organizational information systems and any associated information system connections; and*

(iv) *monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.*

Ensuring the effectiveness of security controls and the ongoing protection of organizational information systems is critical to maintaining the confidentiality, integrity, and availability of sensitive data. This chapter focuses on the certification, accreditation, and security assessments processes that facilitates the periodic evaluation, authorization, and continuous monitoring of security controls to mitigate risks and enhance the resilience of information systems.

5.1 Periodic Assessment of Security Controls

Regular and comprehensive assessments of security controls are essential to identify weaknesses and vulnerabilities within organizational information systems. Key aspects of periodic security assessments include:

- Regular and comprehensive assessments of security controls
- Procedures for evaluating security controls
- Documentation, analysis, and reporting

For all of our security controls and systems we need to conducts tests and assessments on them. This is to help ensure there are not any noticeable weak points, vulnerabilities, or failures. Every so often, and particularly with any updates to systems, we need our security personnel to stress test the systems with common forms of attacks on each one to ensure that is will not easily fold in production.

For evaluating the protocols and systems we have in place, we need to schedule when all tests take place. This is because we do not want to randomly test our systems and accidentally

shut them down during the busy hours of the day and lose productivity. For some of our systems that are tested during the day, we do not want to attack the entire set of servers or systems, since they must remain operational.

All findings of these tests should be documented so that we have a comprehensive notes of what was tested, when it was tested, and how it was tested. All findings will be useful in providing insights for informed decision-making and strategic planning when an security event does occur.

5.2 Implementation for Reducing Vulnerabilities

Efficiently reducing vulnerabilities in our company's systems and servers requires a systematic approach to identify, prioritize, and address security weaknesses. Some concepts for finding and reducing vulnerabilities include:

- Process for identifying and prioritizing vulnerabilities
- Development plans to mitigate or eliminate identified risks
- Monitoring of corrective actions and mitigation measures

During the periodic assessments phase, it is likely that vulnerabilities will be found and documented. When this occurs we need to categorize them in a priority list since it is unlikely that a small amount of vulnerabilities will be listed and effective management of them is necessary. When they are documented we need to asses how likely the vulnerability could be triggered and if so how much damage it could cause. Primarily the damage it can cause will get the item a higher priority for fixing it. Although a very common, but small damaging vulnerability might also get a high priority, but it all depends on the situation and the best judgment of our security experts.

With the list of known vulnerabilities we need a plan for tackling them. It is heavily advised that all high risk items are fixed as soon as possible, ideally within the same day they are identified. If it is not high risk then we want to ensure a timely fix for all other items so that they will not become a problem in the future. Like with the assessments done earlier, all fixes will need to be adequately tested to ensure they will mitigate the vulnerabilities that they are trying to fix without creating new ones.

After the items are identified and prior to them being fixed, it is important that they are being closely monitored. We do this because if we know where risks are located at, then we know what a likely cause of attack could be if one occurs. This useful because then it will be easier to identify and for our personnel to be aware about. We also need to monitor the progress of the fixes, since any high priority items need to be fixed quickly but they also need to be up to a good standard to not introduce any new problems.

5.3 Authorization of Information System

Authorizing the operation of our company's information systems and associated connections involves assessing compliance with policies, regulatory requirements, and risk tolerance levels.

Key components of authorization include:

- Review, approval, and documentation of authorization decisions
- Risk acceptances, and authorizations based on compliance with policies, regulatory requirements, and risk tolerance levels.
- Periodic re-authorization of information system

It is crucial that we are reviewing, approving, and documenting authorization decisions because we need to know who, what, and when items are being authorized by. This also plays into keeping logs of everything so that if an incident were to occur either during or after these approvals, then we know exactly where to look to correct the issue. Then we can also inform those involved to ensure that the issue does not happen again in the future.

We will also conduct periodic re-authorization of information systems to maintain compliance and effectiveness of security controls over time. Like with our access controls, we need to reset items every so often just so it forces us to reevaluate the items we have in place to see if any changes are needed.

5.4 Continuous Monitoring of Systems

Continuous monitoring of our programs, processes, and tools are essential validating the effectiveness of our security protocols on an ongoing basis. Components of our monitoring protocols include:

- Implementation of continuous monitoring
- Reporting, analysis, and communication of monitoring results

Since we manual monitoring will not properly allow us to have continuous monitoring, we need some automation with our monitoring system. For all of our information system security controls we need automation on it with either intrusion detection systems or intrusion prevention systems. This way we can leave time and resources of our personnel to work on other important items rather than just watching our systems logs and traffic all day. Additionally, if setup properly, this will reduce the chance of human error from missing an item that should have been detected.

From these continuous and automated monitoring systems they need to be reporting and analyzing results and trends to enhance risk management and decision-making processes. We can easily make our detection systems analysis the data its receiving and make well-informed decisions on if there is a potential threat that should be addressed.

Chapter 6

Configuration Management

(i) *Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and*

(ii) *establish and enforce security configuration settings for information technology products employed in organizational information systems.*

Configuration management is important for upholding the integrity and security of our systems, servers, and data across the organization. It serves as a foundational pillar in our security framework, enabling us to greatly limit risks of malicious software and unauthorized configurations within our information systems. It is crucial we have these configurations setup initially to prevent someone from accidentally bringing a virus, worm, or some other type of malicious software into our systems.

6.1 Baseline Configurations

Creating and enforcing our baseline configurations and inventories of organizational information for all systems and devices in our company happens the moment we get the device. To set up these configurations there are two main components to follow.

- Device Registration
- Approved Software

Every device within the company is registered and undergoes initial installations of approved security software and configurations to restrict general user access. This process establishes our baseline configurations for all devices, enhancing security and lowering the risk of malicious software. We need to essentially restrict the ability for users to just freely download anything from the internet as that can be a weak point if someone is not careful. As well as we need to add our virus detection software and monitoring systems to properly audit and log actions the users are taking with the permissions they have access to.

Since free range to internet downloads is restricted, we need to identify software utilized across the company. This enables the creation and documentation of an approved software list and an internal application to install these items from. This list contains validated versions of essential programs and software, ensuring consistency and mitigating the risk of unauthorized installations. Users can access these approved programs through a designated app portal installed onto their computer during registration. This is to reduce the likelihood of unauthorized software compromising system integrity.

6.2 Security Configuration

Any programs that are needed for a task that is not already in the list of approved software must undergo an approval process before being added to the approved software list. This process involves a business case from the employee(s) or team that need to use it and the software with its version information. As well as that the validation process includes:

(a) Ensures programs are downloaded from reputable sources

(b) Establishes trust in service providers

(c) Verifies the absence of known vulnerabilities in the version requested

We need to the programs to be from reputable sources, like for example, if a specific IDE is needed for development of a specific application, we need to find the correct source for downloading the software. For example, if it is a JetBrains IDE, we need to locate the download to the JetBrains products page.

On top of this, we also need to verify that the version number we want to install is validated and tested so that any known vulnerabilities with it either do not exist or will not cause problems with anything on our systems. This validation procedure is also done for all applications in our approved list whenever updates become available to them.

All of these steps are needed to help ensure that the program can not and will not increase the likelihood of any malicious software from comprising the confidentiality, integrity, or available of our systems, servers, or productivity.

Chapter 7

Contingency Planning

Establish, maintain, and implement plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Contingency planning is a critical component of organizational risk management, ensuring that our company can effectively respond to and recover from unexpected events or disasters that may disrupt normal operations. This chapter outlines the principles and practices involved in establishing, maintaining, and implementing contingency plans for emergency response, backup operations, and post-disaster recovery of our organizational information systems.

7.1 Emergency Response Plans

In the event of an emergency, a quick and effective response is important to help minimize disruption and safeguard our personnel and assets. There are many different types of emergencies that could occur and the response for each can vary. Some examples of emergencies are:

- Natural Disasters
- Security Incidents
- Physical Security Breaches

In the unlikely-hood that a natural disaster occurs and significant damage has been done to our company's assets, we have one main response plan. If the buildings are damaged in any way we will need to evacuate and recover what we can from the remains. Then we will need to relocate the operations that took place in that area to a new, temporary location while reconstruction takes place. In the case where our servers and data get taken out, it may take a while before operations continue, as new servers will be needed and our method of data backup recovery will need to take place.

When a security incident occurs, prompt and clear communication is essential to mitigate further damage of our company's assets. It is crucial to immediately notify all employees and security personnel affected by the incident, utilizing a notification system (i.e email) to ensure proper communication of the situation. Alongside this notification, clear instructions must be provided, stating the importance of locking down any potentially compromised systems. Employees with these compromised systems should be told to refrain from accessing or modifying

sensitive data, while the proper security personnel try and stop the ongoing threat. Throughout the incident response process, communication channels will be established to provide regular updates and status reports. Once the incident is resolved, it is crucial that we communicate any lessons learned to all employees and security personnel, reinforcing the importance of adherence to security best practices to help prevent future occurrences of this incident.

When a physical security breach is in place, more specifically a violent security breach, immediate action is essential to ensure the safety of all individuals within the building. The entire facility will be placed on lockdown and all employees will receive a notice directly through the building's intercom system or an alarm system specifically designated for such emergencies. These protocols are taught in each employee's yearly required training, which mandates their compliance in learning these procedures. While all personnel are instructed to prioritize their safety by following our lockdown procedures, be vigilant and responsive to any security officers and relevant authorities. All of which will be promptly notified to respond and manage the situation effectively.

7.2 Backup Operations

Protecting our company's data is a top priority, and backup operations are essential to ensure its availability and integrity. Our backup operations are designed to mitigate the risk of data loss and facilitate timely recovery in the event of data breaches, system failures, or other disruptions. Key aspects of our backup operations include:

- Importance of regular data backups
- Frequency of backups and locations
- Testing and validation of backup procedures

We perform regular backups of our critical data to minimize the impact of data loss and support timely recovery efforts. It is important to us that we spend time to backup our data periodically, so if data is lost or corrupted for one reason or another, it becomes possible for us to get a backup copy.

Backup frequency and locations are other items we need to consider, if all of our data is only stored in one physical location, then if the building gets taken out the backup procedure will fail. Meaning we need to have at least a second location to store all of our sensitive and important data we have for our company. Ideally, the second building is not near the first one for the sake of severe weather. It is important that all locations are getting the all the same frequent data backups.

Our backup procedures undergo regular testing and validation to ensure data integrity, and accessibility, all so that we are all to successfully recover it. We will conduct simulated recovery exercises to verify the effectiveness of our backup systems and procedures in real-world scenarios. These tests will be regular just like with any other security testing and maintenance that is done.

7.3 Post Disaster Recovery

Recovering from a disaster requires coordinated efforts and decisive actions to restore operations effectively to help minimize downtime. Our post-disaster recovery plans are designed to facilitate quick recovery efforts, enabling us to resume normal business activities as quickly as possible. Key elements of our post-disaster recovery plans include:

- Recovery Strategies
- System Prioritization
- Monitoring
- Lessons Learned

For the post disaster strategies that we have, it'll depend based on the severity of the situation which is enacted. The following data solutions that can be used:

- Data center failover to secondary location
- Cloud-based data recovery
- Data restoration from backup centers

Most of the time a data backup from a secondary location will be the easiest for us, but in case that is not possible, utilizing cloud services would be another great options for us.

We also need a prioritization list of what items we need to recovery first. First and foremost our company's sensitive and important data that all operations run on is the most important asset to us. Next any company servers that are down are next to recover, we need are internal servers running for any of our products to be available publicly. Finally, any remaining business operations that are for the public need to be fix, so that everything can get back to normal.

During the recovery process we closely monitor everything that is ongoing. We do this by tracking milestones, identifying bottlenecks, and adjusting recovery strategies as necessary to meet our objectives in a timely manner. We also do this in case there are any follow up disasters or any other potential threats that might be trying to break their way in when we may be more distracted.

Lastly, any new lessons learned from the recovery process are documented to help improve future contingency planning efforts.

Chapter 8

Identification and Authentication

Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

The implementation of a robust access control and authentication system is an integral part in keeping our company's systems and data safe. This section goes into the intricate framework that governs who should have access to different sets of information and the reason behind them. The emphasis on need-only basis and the inclusion of authentication framework contribute to the success of our security protocols.

8.1 User Authentication

The reason these security protocols must be enforce have to do with a lot of potential weak points that could cause lots of confidentiality, integrity, and availability issues. Some Items in particular that will be targeted to protect against:

- Protection of Confidential Information
- Prevention of Data Breaches
- Ensuring Business Continuity
- Protection Against Cyber Attacks
- Protecting Intellectual Property

These items in particular are our top priority to protect. This is because if we have any data breaches and our confidential information gets leaked publicly, then a lot of personal information of either our customers or employees is now available for everyone to see. This type of data leak would do catastrophic damage to our company and it reputation likely putting it at risk of being shut down. We also want to prevent different cyber attacks so that our systems do not go down, because if they always get taken out or compromised then we can keep our normal business operations going to be profitable.

8.2 Password Policies

The most common method of user authentication is password-based authentication. Users are required to select a unique password, which they must provide to gain access to the system.

Though password-based systems are the most common they also have their own vulnerabilities associated with them. To help mitigate some of these vulnerabilities we will use hashed passwords and have a set of requirements that all passwords within the company systems will have to adhere to.

8.2.1 Complexity

Passwords must adhere to a set of requirements to enhance their strength by increasing the complexity of them. The addition of more characters in a password greatly increases the time required for someone to brute force their way into an account. More specifically, everyone must satisfy the following conditions:

- At least one or more uppercase characters
- At least one or more lowercase characters
- At least one number
- At least one special character
- The use of commonly guessable information, such as names, is discouraged

Though even with these requirements we do not want to make passwords too complex that employees have trouble remembering them. This is because the likelihood of employees writing them down will significantly increase and that in itself is a security risk, especially if it is not in a secure location. This shifts our goal from strictly eliminating easily guessable passwords to also make sure that everyone can make memorable passwords for themselves. A good technique for choosing a password is to use the first letter of each word of a phrase. Studies have shown users can generally remember such passwords, but they are not susceptible to password guessing attacks based on commonly used passwords.[1]

[1] Refer to Appendix A.1 for source.

8.2.2 Length

To help reduce the time and chances of someone being able to crack a password a minimum length will be enforced to help add another layer of security. Longer passwords greatly increase the difficulty for attackers that will utilize any sort of brute force method for password guessing. For all employees and customers the following will be enforced:

- Minimum length of 12 characters
- Longer passwords being recommended

For our passwords with a minimum length of 12 digits and with the complexities explain previously, it would take a computer nearly 34,000 years to brute-force an individuals exact password.

[2] Refer to Appendix A.2 for source.

8.2.3 Password Expiration and History

Since passwords can be compromised often without anyone knowing its best to have password expire after a certain period of time to prevent the chances the stale, prolonged password becomes more of a security risk. This means a policy of password expiration will be implemented.

- Passwords will need to be changed every 180 days
- This applies to all accounts and devices
- Will be prevented from reusing passwords from the previous 2 years

Though, if we know we have compromised passwords we can change the expiration date for the compromised users to force a password change as soon as possible. If the password is not changed by the expiration date of it, then there will be an initial grace period, but after that is up, the account will be locked out or force a password change upon the next login with the user.

8.2.4 Account Lockout

To further help prevent brute-force attacks, accounts will get locked if there is 5 consecutive failed login attempts for an account. The owner of the account will have to contact the IT department to unlock their account by proving their identity which will result in their password being reset.

8.2.5 Multi-Factor Authentication

For the extra layer of security and keeping everything secure employees will have to set up multi-factor authentication (MFA) when they login. This extra layer helps prevent unauthorized individuals from attempting to login with someone else credentials. All employees can use their personal phones as the source for MFA.

8.3 Biometric Authentication

Biometric authentication leverages unique physical characteristics like fingerprints or facial features as another layer of security. Given the complexity of maintaining long and intricate passwords for device security, employees are encouraged to utilize available biometric login options if their devices support them. This will help increase a user-friendly experience whilst also keeping their devices secure whenever someone may step away from their desk or move their computer around. Since passwords are still required for devices having biometric logins enabled, they will still need to know and use the password whenever the device deems it necessary.

This option will be restricted to device logins only. Allowing biometric authentication for all services and systems could elevate the risk of a security breach by centralizing biometric information in our databases and servers. Instead, leveraging the built-in security measures and protocols of the devices ensures both a high level of user experience and overall security.

8.4 Identifying Users

On top of the password requirements for identifying a user we also need some other metrics for identification. To accomplish this we can use digital signatures, which can be used to provide authentication, integrity, and non-repudiation for messages exchanged between users, processes, or devices. Some of the different items that will be used will be:

- Digital signatures
- Public-key certificate
- Symmetric key exchange
- Digital Envelope

The digital signature will be able to provide authentication, data integrity, and non-repudiation. Each user will have a public key which is binded to their identity and which enables us to use symmetric key exchange using the public-key encryption protocols to give us our digital envelopes. All of this is done for the sake of sharing documents and messages between different parties to help ensure data is not compromised.

8.5 Account Creation and Management

Something that needs to be addressed is the management systems for the accounts of each personnel within the company. For each new user a new account must be created and must have a default secure password that is given to them so they can reset it upon logging in for the first time. Otherwise, it can be a huge security risk when new employees are added and someone figures out the temporary password.

Accounts must be manually and automatically managed as well. This is done for the sake of knowing when the system should lockout an account, or to know when to delete an account that is no longer needed. Employee termination is the likely cause for deleting an account that is no longer needed. As well as a temporary account lockout could be utilized if an individual is take an extended leave of absence from the company since we do not want their credentials to be used by an unauthorized source.

8.6 Processes and Devices

For all work-related activities done within the company, employees are required to utilize only company-provided devices. The idea behind all this is to ensure the implementation of additional security protocols embedded within company-issued devices. This software helps keep the device operation under the company VPN, which mitigates potential security risks. Ideally, this policy aims to improve the security of internal and confidential data from unauthorized access.

It is also important to note that external devices are prohibited from connecting to any company-provided device. Some examples of items that should not be connected are, but not limited to, the following:

- External USB sticks
- External storage device
- External phones

The reason this is not allowed for the general population is that if an external device is unregulated or not secure there is a chance a worm, virus, or some other malicious attack could be present on these memory devices. If there is a need for a device to be connected to a computer a business case must be made. Once approved the company will provide the external device that will be allowed to be connected.

8.7 Data Encryption Protocols

Data encryption is a big deal when it comes down to keeping lots of confidential information safe and secure from outside attackers. It is important that the sensitive information is kept under a robust set of data encryption protocols. Doing so would essentially render the data useless to unauthorized users as they would have no way to interpret or read the data if they manage to get a hold on it.

In order to keep this data encrypted there will need to be a few different protocols in place for the different type of data that is encountered and dealt with.

- Encrypt data in transit using secure communication channels and encryption methods
- Encrypt data at rest using approved encryption algorithms and mechanisms
- Protect encryption keys from disclosure, loss, or compromise using key management systems and practices

Chapter 9

Incident Response

(i) *Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities; and*

(ii) *track, document, and report incidents to appropriate organizational officials and/or authorities.*

Establishing an effective incident response effort is crucial for adequate detection, analysis, containment, and recovery from security incidents that may cause damage to us. This highlights the key components of our incident-handling capabilities to ensure an effective response to any and all security incidents.

9.1 Preparation

The first and most important initial step is to have policies and roles in place to handle any security incidents that will occur. We need to list out all items that could be a cause of an security incident, this includes anything from employee mistakes to sensitive documents we keep on record in our systems. We also need to prioritize the different incident that can occur so in case there are multiple problems at once, we do not need to think about which is of higher importance.

Now in order for this to be successful across the organization we need specialist in handling these incidents apart of every team we have. These individuals can be apart of multiple teams, but we must have enough around that can be ready whenever an incident is detected. Individuals in these roles will also be the ones testing our security systems to ensure they are up to par, but that discussion is in another section of this manual.

The last part for this preparation is having techniques in place to prevent a lot of incidents before they can occur so our specialist can spend there time working on problems that may not be easily preventable or foreseeable. An intrusion prevention system (IPS) or an intrusion and detection system (IDPS) would be a great way to prevent a lot of overhead that could potentially be a threat to our systems.

Some items that can be used as an IPS are:

- Host-Based IPS
- Network-Based IPS
- Distributed or Hybrid IPS
- Snort Inline

The host-based IPS can be used for monitoring a single host's characteristics and events to identify and stop an potential suspicious activities. This is done based on behavioral analysis and network filtering to monitor any running process, files, etc. This is useful since we can have it be on any sort of device or server within the company to help prevent someone from doing any potentially dangerous activities.

A more general prevention system to put in place is a network-based IPS, which is a device or software that monitors traffic passing through a network. These are installed at the network's perimeter to monitor all traffic that enters and exits the network. This can greatly lower the risks of attacks on its own since it sees everything going through out network, meaning we can block and filter out a lot of the initial spam or suspicious items before it can even reach out servers. One of the main things a network-based IPS prevents are threats such as denial of service attacks.

Distributed or Hybrid IPS solutions represent an approach to intrusion prevention and detection by integrating the capabilities of host-based and network-based IPS into a unified and centralized security architecture. We can utilize a balance of both systems in order to have a variety of methods to be able to prevent lots of suspicious activities that can take place through the network and on each individual host.

Snort inline is an extension of Snort, which is an intrusion detection system that gets extended into also provide intrusion prevention features. These three features are drop, reject, and Sdrop, which essentially are 3 different ways to filter out packets with different actions for taking care of them.

9.2 Detection and Analysis

In order for the detection to be effective, we need to implement the proper systems and tool in order for it to work. For our operating systems we will need to add different anti-viruses and host-based firewalls and even intrusion detection systems. This is what NIST SP 800-123 suggests for basic protections for the operating system, like our company computers as an example.

As for our implementation, we need to configure continuous monitoring tools to generate alerts for suspicious activities. To do this there are many different things we can automate the supervision of, some of the items are:

- Data collection
- Analysis processes
- Rapid detection and analysis to incidents

For data collection, it involves gathering information from various sources which include logs from our servers, network traffic data, system events, and more. Utilizing tools such as loggers and network monitoring can help automate the collection process. By centralizing and standardizing data collection, we can ensure comprehensive coverage and easier analysis.

Once the data is collected, it needs to be analyzed in order to be identified as potential security threats. The analysis we do will utilize strategies such as pattern recognition, anomaly detection, and behavioral analysis. These automated processes will be designed to identify both known threats based on predefined signatures and unknown threats based on behavior anomalies.

The goal of our data collection and analysis is to quickly identify and respond to security incidents to minimize their impact. These two items will then allow us to have rapid detection to any potential threats which allows us to go in and stop or prevent the problem from getting worse.

For the analysis side of things, we need to establish a tiered incident classification system and corresponding response procedures tailored to each category. This is to help facilitate and to ensure consistent and timely handling of security incidents based on their potential impact on our operations and data. The tiers would be as follows:

- Low
- Medium
- High
- Critical

Each level of impact a threat is will have a window of how urgent it is and how quickly the teams should try and resolve the issue depending on the severity. For low, the incident would be minor, and is not likely to be exploited or the exploit does not have a huge effect on the company systems and data. Low rated items would be taken care of as soon as capacity is open for someone to do so. Medium are items that could become more common or be able to have a more moderate effect to are company. These items should ideally be taken care within 24-48 hours. High level vulnerabilities, could have significant negative impacts on the company, and should be taken care off within the day the item is discovered. Finally, critical level items could have non-fixable damage depending on the severity of the attack or attacker. These items should be taken care off immediately upon discovery. It should be noted, that severity levels can change for any outstanding item or if more information is discovered about it.

9.3 Containment

When a security incident is detected and requires a response no matter the severity level, we need likely will need a way to contain or neutralize the incident before being able to prevent it from occurring again. It's at this step where documentation starts to become a vital thing to be completed. This is because if we have similar events occur in the past then people can reference our documentation to see what the exact procedure was to stop the problem, this can help speed up the containment period.

Some steps to help contain and isolate an incident is:

- Documenting step-by-step procedures for affected systems
- Disabling compromised accounts
- Blocking malicious IP addresses
- Utilizing firewalls to restrict traffic
- Monitor isolated systems for malicious activity

Creating detailed documentation of step-by-step procedures for responding to security incidents is crucial for efficient and effective containment. This documentation needs to include instructions for identifying indicators of threats, isolating any affected systems or servers, and implementing recovery measures. This will allow for our security experts to quickly be able to mitigate any threats or incidents when they occur or reoccur, if not previously documented.

One of the immediate actions to contain a security incident involving unauthorized access is to disable any affected user accounts. This prevents further unauthorized activity from the affected accounts and allows the security personnel time to fix the issue.

If the security incident involves malicious incidents from external threats, allowing security personnel to block any associated IP addresses can help prevent further malicious activity. This will be done by updating our network firewalls or our intrusion prevention systems if it needs to be automatically filtered out. This is why firewalls play a critical role in containing security incidents since we can control any network traffic.

After we isolate any affected systems during the containment process, it is important to continuously monitor them for any future signs of malicious activity. This can involve intrusion detection systems or solutions to monitor system logs and behavior. By actively monitoring isolated systems, organizations can detect and respond to any attempts by threat actors to escalate privileges, spread laterally, or further compromise the environment.

By elaborating on how each containment step can be utilized within your incident response process, you provide a clearer understanding of the actions required to contain and mitigate security incidents effectively.

9.4 Recovery

For post-disaster recovery or recovery of any sort of successful attack, we need procedures in place to help identify what must be done to move forward. This includes processes for restoring any affected systems or data, and being able to get the company assets back to normal operation as soon as possible. Once the attack is over and contained, depending on what was affected here are some items that need to be checked to get everything back to normal.

- Restart any servers taken offline
- Restore any compromised data from backups
- Validate system integrity
- Verify effectiveness of implemented controls

First and foremost for recovery, likely any items taken offline will just need a reboot as a good starting point. Then if any data was comprised, deleted, or tampered with in some way, assuming we can, we need to go to the data backups and put the information back out that we know is safe and accurate. Next we need to go through and test our systems to see how our systems were compromised and identify what actions need to be taken to ensure that an attack like that can not be repeated in the same way.

9.5 Tracking and Documentation

For every incident that occurs within the company, we need to track it. The idea behind this is that we want to have history of every incident that occurs no matter how big or small. This helps us be able to know everything that has happened and when it occurred as well as being able to document everything about it so we know how to fix/prevent future cases that are similar. to do this, implement a centralized incident tracking system or database to record, categorize, and archive incident-related information.

On top of the tracking of each incident we also must document everything about it, this will help us out a lot when it comes down to fixing other issues and prevent the same thing from happening again. Everything and anything related to the incident should be noted in the report that is created after the fact, questions we need to ask ourselves are:

- How and why did this occur?
- Was this preventable?
- Has something similar happened before?
- How did we resolve this issue?
- What other information is related to this incident?
- Are there any trends occurring with this incident and other recent or related ones?

All of these questions must be answered in each report and when documentation the incident. As well as any other important or relevant information that is not directly stated in the list above should also be included if applicable. The more detailed our documentation is and easier the accessibility to reference it all, the easier it can be to resolve any issues that occur in the future.

Chapter 10

Maintenance

(i) *Perform periodic and timely maintenance on organizational information systems; and*

(ii) *provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.*

Regular and timely maintenance of our systems and servers is crucial to ensuring their optimal performance, reliability, and security. Effective maintenance practices not only mitigate the risk of system failures but also contribute to the overall resilience of our infrastructure. This chapter explains the principles and procedures for conducting maintenance while maintaining control over tools, techniques, mechanisms, and personnel.

10.1 Periodic and Timely Maintenance

Scheduling regular maintenance activities is crucial for proactively identifying and addressing potential issues before they can escalate into problems. For all of our systems, servers, devices, and any other company-wide software, we need to have regular maintenance and updates when deemed necessary.

For all company issued devices, everyone will get a notice when a new security patch or security update is available and the deadline for them to complete it by. If this update is not completed prior to the deadline the device will force the update to be completed, or else the device could be locked if that does not succeed.

For our systems and servers however, we will only update them when it is important to do so. For example if an hardware or software update is required for a huge security patch, then we will schedule a time, likely over-night, to completed the required maintenance of all the systems that require it along with a estimated time frame to complete this. When these windows are scheduled and if all of the servers all need to go down, proper notices will be place out publicly and/or internally depending on what specifically is impacted. This includes routine checks of hardware and software configurations to ensure their proper functionality.

It is also important to monitor and document all the the maintenance schedules and performed as well as the time it took to complete it. We do this because if we start noticing a new issue we can check when the previous updates were to help see if that new update introduced any new threats or issues, meaning we can then revert the changes. This also allows us to get a better idea over time how long different tasks take to complete so when maintenance is scheduled we can have more accurate estimation windows.

10.2 Providing Effective Tools

Equipping maintenance personnel with appropriate tools is essential to have efficient and effective maintenance activities. This includes us giving maintenance personnel access to diagnostic tools, troubleshooting utilities, and software management systems relevant to our systems. Along with this however involves implementation of access controls and permissions helps restrict unauthorized access to these tools and systems, reducing the risk of misuse or malicious activities. Our role-based access controls ensure that only authorized personnel can access sensitive maintenance functions, mitigating the threat of insider threats or unauthorized system modifications.

Monitoring and auditing mechanisms will be implemented to track maintenance activities and detect any unauthorized behavior. This includes logging maintenance actions, capturing system changes, and conducting regular audits to verify compliance with maintenance procedures and security policies.

Chapter 11

Media Protection

(i) *Protect information system media, both paper and digital;*

(ii) *limit access to information-on-information system media to authorized users; and*

(iii) *sanitize or destroy information system media before disposal or release for reuse.*

Media protection has a range of different types of strategies aimed at mitigating risks associated with both physical and digital forms of media. This chapter outlines key principles and practices to ensure the effective protection of our companies digital and paper media.

11.1 Protection of Media

In order to protect our media we need different security measures for both paper and digital copies of our data. Some of our protocols we need to have are as follows:

- Encryption of digital media
- Physical locks on files and systems
- Regular monitoring and auditing of media handling

For all of our data servers and data storage of sensitive data, we need to have encrypted hard drives so they can only easily decrypted by us in case anyone gets unauthorized access to them. The data we want to store here is anything that is sensitive customer data and sensitive internal data that is all saved into our servers and systems.

On top of encryption, for both physical and digital media, we need to keep the information secure and only allow authorized access. To safeguard this information system media,we must implement physical and digital security measures. Physical security measures include secure storage facilities, restricted access areas, and surveillance systems to prevent unauthorized access to physical media. For any digital media, anything in file cabinets or storage areas for paper copies of data need to be protected by different locks or card access room with only authorized personnel able to directly go and access this information.

In these rooms where the sensitive information is stored, we also want surveillance. This can help identify who was in which room and when they were there in case any security incident occurs which can help further mitigate the issue, if they occur. Regular monitoring and auditing of media handling procedures are essential to identify and address any security vulnerabilities promptly.

11.2 Limiting Access

Like with many other spots of this we want to limit access to only those we need it. We need to have mechanisms in place to only allow certain personnel to access the physical copies of any data we may have of either our employees or customers we have.

- Authentication mechanisms
- Regular review and updating of access rights
- Monitoring and logging of access activities

For the different storage areas of the data we need to have card access to the rooms themselves so only a specific set of people can get into the room. On top of this, certain bits of sensitive data will also be locked via physical keys in their respective filing cabinets or likewise objects. These keys will be distributed to those only those who need the different types of data.

We also need to have regular reviews and updating of access rights when necessary to align with the roles and responsibilities of all our personnel. As well as ensuring keys are collected for those who have physical keys. Though this does not always prevent duplicates from being made or any other outstanding keys not in our possession. Since this is an issue that can occur, we will also periodically update all the locks and change the keys every few years or when there is a potential security threat with them.

As stated in the previous section of this chapter we will have surveillance in each room as a method of logging who is doing what in each room, as well as logging the users who key card into different rooms which the IDs and timestamps of when these events occur. This monitoring and logging access activities enables us to track and investigate any suspicious or unauthorized access attempts effectively.

11.3 Information System Media Disposal

Proper disposal of information system media is crucial to prevent the inadvertent disclosure of sensitive information. Because of this, we have some protocols in place to help properly dispose of data in both physical and digital forms.

For any physical, or paper, documents that we have that need to be destroyed, the easiest and quickest solution is to shred the papers, then the contents will be recycled. This is satisfactory for us because if someone is able to put together a full document in the thousands of pieces of paper, that person would not be getting as much out for the time they put in.

Furthermore, we will implement training programs to educate employees on proper media handling and disposal practices, emphasizing the importance of safeguarding sensitive information throughout its lifecycle.

Chapter 12

Physical and Environmental Protection

(i) *Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;*

(ii) *protect the physical plant and support infrastructure for information systems;*

(iii) *provide supporting utilities for information systems;*

(iv) *protect information systems against environmental hazards; and*

(v) *provide appropriate environmental controls in facilities containing information systems.*

In the realm of security of our servers, systems, and data centers, safeguarding them goes beyond digital defenses. It also includes detection, prevention, and recovery policies against physical and environmental threats. This section explains the proactive measures implemented to fortify our systems against intentional, accidental, and unavoidable actions that could jeopardize their integrity and availability. From strict access controls and surveillance systems to environmental monitoring and disaster recovery planning, every aspect is designed to mitigate risks and ensure nearly continuous operations.

12.1 Physical Protection

The physical environment poses numerous risks, often due to human error (both by accident and intentionally). For instance, servers being unplugged by personnel can lead to power loss. To mitigate such issues, several considerations are essential:

- Servers must be physically separated and locked from personnel workspaces.
- Wiring should be isolated for servers and clearly labeled for each item for identification.
- Office equipment on desks, like monitors and charging stations, should be organized with proper cable slack to prevent accidental disruptions.
- Cables should be neatly tied around desks to prevent tripping hazards.

12.1.1 Limiting Physical Access

Referring back to a key concept in the security system from earlier is access control. Like how we have systems in place for a ”need-only” basis when it comes down to digital access, we must do the same for our physical environment as well.

Some key concepts that will need to be in place are the following:

- Access Control
- Perimeter Security
- Visitor Management
- Surveillance Systems

For our server and data center rooms, the entry points into them must be locked and can only be accessed through authorized key card entry. This means only personnel who work on the severs and data centers have can enter the rooms to perform maintenance or any other tasks that need to be done. This however is not the only limits, to enter the building and office space only employees with their keycards can even enter the building, this is to prevent unwanted or unwarranted visitors that may have malicious intent.

All keycard access points will be logged so if for whatever reason a system is compromised by a physical access point we know who's card got into it so it can be locked. If for any reason there are guest entering the building that do not work for the company, they must at all times be accompanied by an authorized employee that does work here. Prior to their entry they must get a guest pass from the front desk before they can leave the lobby area.

For the surrounding perimeter and inside of the building there will be surveillance systems that cover all entry points and inside secure rooms, since this is a good way to detect who was where in case of an emergency. On top of all this as part of the required training for all employees everyone will have a building security section which highlights the importance of their key cards and to not allow others into the building if they do not have their keycard.

12.1.2 Support Utilities

Because the servers and systems will always be running they require some other utilities to help keep them always running without crashing or breaking. The items that will be addressed are as follows:

- Power Availability
- Cooling Systems
- Water Leak Detection
- Fire Suppression
- Monitoring

First and foremost is that the systems must be up and running at all times. To accomplish this we need to have our constant power supply that enough to handle all the systems and servers that we have running. Ideally, this system will be used all the time and never need any other supply, but sometimes we do not have control over those external factors. In case of an outage for whatever reason, we also need backup batteries or generators. This is to keep the systems online for a short period of time until our main power supply is back online. Alternatively, if severe weather took out the power then these systems will then be used to backup all the data to prevent any data loss.

Since these systems and servers take a lot of energy to keep running at all times, they tend to overheat. To help prevent them from overheating and shutting down the server rooms must be properly cooled down to keep the servers at a sustainable temperature. Some ways to handle this are air conditioning that has the only purpose of cooling the server rooms as well as proper airflow management. If implemented correctly, these items will maintain the optimal temperature levels needed.

Water can be a huge detrimental object that could present itself without anyone expecting it. Because of the huge negative impact it could pose, we must have the server room be in a spot that is designed to prevent a water leak or potential flooding. On top of this, we will need a detection and prevention systems in place in case any water does find its way into the server rooms. If these exist then we can be more proactive about keeping the servers and systems online and mitigating any other issues if a problem does occur.

Likewise to water, we also need fire detection and suppression. In each server room smoke detectors are a requirement as that is just a building code safety standard. Although we need to be careful with the suppression system, fire extinguishers will be present but we need an automated system which can help start the fire immediately upon detection while help is on its way. Ideally, they are in place to minimize any extra damages by putting out the fire.

For all these items mentioned already, one thing that encapsulates them all is a general monitoring system of the server room environment. We need to track temperature, humidity, and other environmental factors in data center facilities, allowing for proactive management of environmental conditions.

12.2 Environmental Protection

Unfortunately, there are factors that are not always preventable. Such items are related to our outside environment, such as the weather or more specifically, severe weather. For our main systems and servers, these items must be taken into account:

- They must be locked in a room that can be considered a ”safe room” for various severe weather events the area could experience.
- Protected from problematic outside attackers or intruders that may try breaking into the building or room.
- Store backup data and other sensitive information securely in fireproof safes or off-site storage facilities to protect against environmental hazards.
- Conduct regular inspections of data center facilities to identify and address any vulnerabilities or weaknesses for inadequate environmental controls.
- Develop and maintain comprehensive disaster recovery plans to mitigate the impact of environmental hazards, ensuring operations are continuing and the timely recovery of any damages.

Chapter 13

Planning

Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Developing comprehensive security plans for our systems, servers, and data is essential to preserve the confidentiality, integrity, and availability of it all. By documenting security measures and updating them to address new threats and vulnerabilities, we can help mitigate risks and keep our confidential data secure.

13.1 Periodic Updates

Our security plans are not fixed rules and regulations but dynamic frameworks that need to response to changing threats. Regular updates are conducted to test the success of existing security protocols and locate emerging risks. Then it can be possible to incorporate new strategies to enhance security of our systems. Improvements and changes of our security plan is a collective effort involving various groups, including:

- IT personnel
- Security experts
- Business leaders
- System administrators

By periodically reviewing and implementing these plans, we ensure that our database, systems, and confidential documents remain safe and secure from new and emerging threats. It should also be noted that this document itself should be continuously updated if any big changes should occur to keep up-to-date with the changing landscape of security.

With each update, its important that any documentation regarding new threats and security protocols are clearly noted. This is important so anyone who needs to worry about security threats can be actively informed in updated training and emails. As well as the engineers knowing what design choices they need to be weary of when their development continues for company products.

Chapter 14

Personnel Security

(i) *Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;*

(ii) *ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and*

(iii) *employ formal sanctions for personnel failing to comply with organizational security policies and procedures.*

This chapter focuses on safeguarding our organization's employees. Ensuring the trustworthiness of individuals in positions of responsibility is paramount, along with protecting organizational information and information systems during personnel transitions. This chapter outlines our methods of a secure environment by implementing protective measures during personnel actions, and enforcing compliance through formal sanctions.

14.1 Background Checks

All individuals occupying positions of responsibility within our organization and any third-party service providers must be trustworthy and meet our established security criteria. These background checks will initially start with the hiring process, but can also be subject to current employees if deemed necessary. These are the general guidelines we will follow, but different roles may be subject to harsher checks.

- Criminal background checks
- Employment history
- Education is verified
- Reference checks (if necessary)

We first need to start with criminal background checks, this is because depending on the role it depends how strict we need to be when hiring an individual to be trusted with our systems. Although the history someone has may or may not be a factor in the hiring process depending on what their criminal history is and how long ago the event(s) occurred. Though this is mainly for the safety of our employees that work as well as the safety to our systems and sensitive data.

Along with this, we also need to verify the employment history that potential employees provide to us and ensure they are consistent. This is because we do not want someone who may try and work multiple jobs simultaneously which the risk of using our confidential information to a competitor or some other company. We also want to verify the experience for each individual, since they must meet minimum qualifications and experience requirements for their positions.

In addition to this, education is also an important aspect to verify depending on the individual, for a fresh graduate we would want to verify the education for a degree-specific role like for our engineer roles. Though the more work experience someone has in a specific field, the less this criteria matters, but it is up to the hiring managers to make those informed decisions.

Finally, for any extra checking that the hiring personnel require, we will use their references, that the potential employee may have provided to help give a sense of confidence before making any decision.

14.2 Protections During Transfers

Protecting our sensitive information during personnel transfers is crucial to maintain security and prevent unauthorized access or data breaches. When personnel transitions occur, whether it's due to transfers within the organization, reassignments to different roles, or terminations of someone, it's essential to ensure that sensitive information remains secure. Our procedures that must be followed in order to have successful transitions are:

- Update Access Controls
- Data Protections
- Equipment and Devices
- Training and Awareness

When an individual is transferring between teams or departments within our company, we need to first review and update access permissions based on the new role and responsibilities to align with the new area the individual will be working. Then revoke or modify access to sensitive information and systems that are no longer required for the transferred role. For example if they had badge access for the servers room and are no longer apart of a team that needs it, we must remove that access they once needed.

If the individual needs certain information transferred from one part of the company to another, depending on the situation, we have to encrypt sensitive data before transferring it to new systems or locations. This will require a method of secure file transfer protocols and procedures to safeguard data during transit. If the physical location of the data needs to be moved, or transferred between networks, it may be safer for us to manually ship all the data across the country to where it needs to go rather than send it through the network.

It it also important to note that different teams may be using different computers or devices depending on the jobs and responsibilities of each team. We need to ensure that all company devices, including computers, laptops, and mobile devices, are collected and securely wiped before reassignment. Remove all personal and organizational data from equipment and devices to prevent unauthorized access. This is important since we do not want someone to carry their device around with potentially sensitive information on it they no longer need to have access to.

When someone is transferring teams, it is important that the individual and the managers are provided with training and guidance on the importance of data protection and security during the transfer process. This is because we want to ensure all parties are aware of the proper protocols prior to a transfer to in order to have a secure and seamless transition period.

If an individual is either leaving the company entirely or being terminated from the company, a lot of the procedures are the same. We need to ensure we retrieve their devices that were sent out to them by the company, since all the information on it will need to be securely wiped to prevent someone from gaining unauthorized access to it. We also will need to remove all accesses and roles to their name within the system and then once everything else in the termination process is taken care we we must remove them from the system entirely.

14.3 Enforcement of Compliance with Security Protocols

In order to ensure compliance of all out security protocols, we must have methods in place to enforce them along with disciplinary actions if someone breaks the rules. For all employees, yearly training will be in place in order to inform and to remind individuals about how to work in a secure environment and protocols for reporting situations that may be deemed unsafe. If an individual is failing to comply with our security protocols to keep everyone and everything safe and secure, a termination system must be in place. This is because ensuring compliance with our security policies and procedures is vital to maintaining a secure environment.

For any individuals that are failing to comply with our policies and protocols, formal sanctions will be enforced. These procedures are as follows:

- Policy Violations
- Investigation and Review
- Monitoring

Anytime an individual violates a security policy we need to document instances where said individual failed to comply with our security policies and procedures. As well as we need to notify them immediately so they are aware of what they did wrong. We want to do this because it is very likely someone may just accidentally violate a minor policy, so no disciplinary actions would follow. This is why we need to classify violations based on their severity and impact on organizational security.

If someone starts to rack up many different violations that have been documented, then it may be necessary to conduct an investigation to gather evidence and assess the extent of the policy violation. It could be the case it is all accidental or maybe they are doing something malicious, it is hard to say for certain without any evidence. During the investigation we must review the findings with relevant stakeholders, including HR, legal, and security teams, to determine appropriate sanctions. From the stakeholders can determine what the correct course of action with the individual is, whether it is termination or extra training.

After an incident is reported and logged we will need to monitor the sanctioned individual's compliance with security protocols. We do this because it can be difficult to tell sometimes if someone did something on accident or intentionally, so to help identify that distinction we add monitoring on those who had a violation. We will also provide support, training, and guidance to help individuals understand and adhere to security policies and procedures.

Chapter 15

Risk Assessment

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Periodic risk assessments are essential for evaluating the potential threats and vulnerabilities that may impact our organizational operations, assets, and individuals. This chapter focuses on assessing risks that stem from the operation of our information systems, which includes processing, storage, and transmission of sensitive data.

15.1 Denial of Service Attacks

A Denial of Service (DoS) attack, is a malicious attempt to disrupt our normal function and flow of any of our services or data by overwhelming it with a flood of internet traffic or other means, making it inaccessible to users. This is a very common type of attack and risk that everyone can encounter since it can be easy to overwhelm services that are not prepared. Which is why we must be able to have our systems and servers setup in such a way to help prevent an issue like this where its foreseeable and vulnerable to attackers. As well as being able to assess the potential risks and find ways to reduce the chances of a Denial of Service attack from being successful. Some negative outcomes to a Denial of Service attack could be as follows:

- Service Disruption
- Data Loss
- Reputation Damage

Service disruption is the most likely outcome of systems and services, which cause operational downtime and loss of productivity. If it's an internal service that is down then the company will lose out on productivity. However if its an external service, like our storefront, then the company will be at risk for losing money, as well as loss of productivity trying to resolve the issue.

If a Denial of Service attack occurs we are also at risk of data corruption or loss. This is a big deal because if our services are down we may not be able to detect data loss right away or how it was lost, and losing this sensitive information would cause lots of damage to the company. This is because it will affect the integrity and availability of our organizational information.

Finally, if services are going out a lot and for long periods of time the societal impact of our organization's image and reputation could be tainted. All due to service outages and perceived security vulnerabilities by the public and it can greatly reduce our customer base.

15.2 Denial of Service Mitigation

There are many ways that we can help mitigate this issue of a Denial of Service attack. Though these will not always prevent a Denial of Service attack they can greatly reduce the chance of many common methods from occurring. Some mitigation strategies include:

- Network Monitoring
- Traffic Filtering
- Capacity Planning
- Employee Device Monitoring

We need to utilize network monitoring since this is a good way to check the flows of everything entering and leaving our network. The way this is used it by continuously checking for something abnormal or patterns that could potentially lead to a Denial of Service attack. As well as that, it can and will be used to detect other malicious items that can occur through our network, but these attacks are the most common.

Another important technique is traffic filtering, we can use this block traffic flow from certain areas around the world or specific domains that are not secure. This will block lots of random traffic that the public storefront does not need and will save company resources and reduce the risk of the servers going down.

Denial of Service attacks can almost be self-imposed accidentally, a big item could be have more than expected traffic to our storefront. There are many reasons why this could be the case, but one which happens a lot for different companies is a big promotion that attracts a lot of attention from customers. If we ever do a big sale or promotion for our companies products then we will need to ensure we have enough computing power to handle all the extra traffic that will come through us for a specific time range.

The last item is especially important as also has to due with the monitoring restrictions talked about earlier in the manual. This is because we do not want a company computer gets a virus, worm, or some other malicious software on the device. If it does happen, it could just be as small as preventing one employee from work, but on the other hand it could go all the way to shutting down our systems. This a good reason why we have these restrictions put in place so that we reduce the chance a wide range of people are affected by a mistake or an internal attacker.

There are many factors to consider when trying to reduce these attacks from occurring. Many of which could happen without a malicious intent, but it is important that we have ways to track what we can to help prevent any easily preventable issues.

15.3 Denial of Service Assessment

For our assessment on Denial of Service attacks there are a few things we need to consider.

- Identification
- Analysis
- Evaluation
- Documentation

In order to assess theses types of threats, we first must know how they can occur within our systems and service. We need to be able to identify potential vulnerabilities and threats, including DoS attacks. This can be achieved through regular security assessments, penetration testing, and monitoring activities. If we do this we can find issues and then prevent them before someone does it by mistake or with malicious intent.

When we go through our identification process, every vulnerability we find we will need to do some sort of analysis on it. This process will include the likelihood and potential negative impacts of these attacks to our systems and services. This is done so we can create a priority list of items so we can spend our time effectively to properly mitigate the more common or more catastrophic problems first. This will also be where the proper strategies and solutions will be analyzed.

After we find and analyze any new threats or vulnerabilities, we must go through and evaluate the effectiveness of our current controls and strategies. This is important since in the world of technology everything changes constantly, so a prevention measure we once used could no longer work after something was updated or a new exploit was discovered. So we must look and find trends with our current measures and see if they are still up to par and we must stay on top of our strategies and see if new exploits are found by other external parties.

This last part is very important, every time we find a way someone can DoS us, we need to document how it can occur and our prevention and/or detection measures we impose to keep it from affecting us. This is all done so we have a comprehensive record for any future reference and so that anyone doing working for us can be adequately trained to avoid certain activities or practices so they do not continue.

Chapter 16

Systems and Services Acquisition

(i) *Allocate sufficient resources to adequately protect organizational information systems;*

(ii) *employ system development life cycle processes that incorporate information security considerations;*

(iii) *employ software usage and installation restrictions; and*

(iv) *ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.*

The acquisition of systems and services plays a pivotal role in the operations and functionality of our organization. However, it also introduces potential risks to the security of our systems.

16.1 Protection of Information Systems

Allocating sufficient resources, including budget, personnel, and technology, will be needed to support the upkeep and protection of our security systems. This is a crucial support team to have funded within our company since they are the driving forces behind developing and maintaining all our of security systems and protocols.

The acquisition process incorporates system development life cycle processes that integrate information security considerations from inception to deployment. Security requirements are identified and integrated into each phase of the SDLC, including planning, design, development, testing, implementation, and maintenance.

16.2 Software Usage and Installation Restrictions

A centralized repository of approved software is maintained, comprising programs and applications authorized for use within the organization. As was mentioned earlier in "Configuration Management", employees are restricted to installing only approved software from the designated app portal. This is for the purpose of reducing the risk of introducing unauthorized or potentially malicious software into the system. For the few business needs where installing software from online is necessary, such privileges are granted to authorized personnel with appropriate permissions. Similar to others however, they may be restricted to only download items from specified websites where it is known to be safe and secure.

16.3 Third-Party Considerations

Prior to any engagement with third-party providers, thorough assessments are conducted to evaluate their security. This assessment of evaluation includes:

- Security policies
- Security procedures
- Security history

This is important to follow as our storefront is an externally purchases entity. Their security requirements, responsibilities, and expectations must be clearly defined and documented in contractual agreements. This is important for the sake of holding any third-party providers accountable for maintaining the confidentiality, integrity, and availability of our company's data.

We also want to ensure that they have a good history, because if they have a tendency to cause a lot of security incidents or increase vulnerabilities we may want to stay away from them. Though this is also situational since there are a lot of factors to consider depending on the nature of the incidents and if they have improved in recent years.

Chapter 17

System and Communication Protection

(i) *Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and*

(ii) *employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.*

This chapter covers some of the main principles that serve as foundational pillars for establishing a robust information security systems within our company. Firstly, it is imperative to monitor, control, and protect organizational communications at both external boundaries and key internal boundaries within the information systems. Secondly, employing secure architectural designs, software development techniques, and systems engineering principles is essential to help prevent unexpected programs from exposing our systems. This approach ensures that information security is an integral part of organizational processes, practices, and technologies, thereby enhancing the overall resilience of our systems and services.

17.1 Firewalls in Organizational Communications

Firewalls are an essential network security system that is designed to monitor and control incoming and outgoing network traffic based on predetermined security policies. They act as a barrier between trusted internal networks and untrusted external networks. Some of the different firewalls are:

- Packet Filtering Firewall
- Stateful Inspection Firewalls
- Application-Level Gateway
- Circuit-Level Gateway

A packet filtering firewall will apply a set of rules to each incoming and outgoing IP packet and then it can get forwarded or discarded depending on the rules that are in place. We can then take this and add stateful inspection firewalls in order to track the state of active connections and make decisions based on the context of traffic flows rather than a fixed rule. For an application level gateway, we can relay application-level traffic, meaning the user contact the gateway and it asks the user for a name of the remote host they want to connect to. Lastly a circuit-level gateway is one that has two established connections rather than just one, the

gateway typically relays segments from one connection to the other. This happens without the contents being examined since the security function consists of determining the allowed connections. That being said, there are many functions that these firewalls will support and help keep secure for our company, such as:

- Access Control
- Traffic Filtering
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Logging and Monitoring

With the different firewall options and functionality available to us, it is important to use the right items for the task. Packet filtering firewalls are good for access control by examining individual packets of data. We do this by basing it on the source and destination IP addresses, port numbers, and other data fields in the packets. This will enforce security policies to allow or deny network traffic based on our static predefined rules, providing a baseline level of protection against unauthorized access.

As stated earlier, stateful inspection firewalls combine packet filtering together with stateful inspection to track the state of active connections. This is done so we can make decisions based on the context of traffic flows rather than checking every individual packet. Thus this makes is effective for traffic filtering since it can maintain high performance and scalability, while still checking for malicious attacks.

Packet filtering firewalls often support Network Address Translation. We do this by translating internal IP addresses to external IP addresses via a lookup table (works both ways). This feature helps preserve address spaces and improve network security by acting as a gateway between different regions inside a network.

Application-level gateways are well-suited for supporting Virtual Private Network (VPN) functionalities. This can facilitate secure remote access and site-to-site connectivity by handling the VPN tunnels and their encryption protocols. Providing enhanced security features and better control over network traffic. Along with this, this means we can have individuals be able to be out-of-office and still be able to securely connect to our servers and work.

Circuit-level gateways are ideal for logging and monitoring purposes. They establish and manage sessions between internal and external hosts, providing detailed visibility into network activities. This is useful since it can generate logs for us and allows us to enable real-time alerts to detect and respond to security incidents effectively.

As explained above each different protocol has its use for different regions in our company to help keep our systems and services safe and secure.

17.2 Software Design Considerations

During the development process of our systems, servers, services, and any other software we deploy, it's crucial to adopt good software development practices. Inadequate testing, overlooking edge cases, or neglecting security considerations can lead to a variety of vulnerabilities, with buffer overflows being one of the most famous examples.

17.2.1 Understanding Buffer Overflows

A buffer overflow occurs when a program writes more data to a buffer (some storage area) than was allocated. This extra data can overwrite other memory locations nearby, potentially leading to system crashes, modifications of system resources, or loss of access control. These vulnerabilities pose significant threats to the confidentiality, integrity, and availability of organizational information systems. Since this issue can occur on any system there are a lot of potential negative effects that could occur from a buffer overflow, such as:

- System Crashes
- Modifying System Resources
- Access Control Loss

Excessive data is one of many reasons a program might crash, disrupting services and potentially leading to unwanted downtime. Overflows can most notably overwrite critical system data or modify the behavior of the program, leading to unpredictable outcomes. This is a huge program since if someone can figure out a malicious input string for example, they might be able to find out information about the system architectural. This then leads to the last point of attackers exploiting buffer overflows to potentially gain unauthorized access to sensitive resources, compromising our security controls and permissions.

17.2.2 Preventing Buffer Overflows

To mitigate the risks associated with buffer overflows, developers should employ various preventive measures and adopt defensive programming techniques:

- Bounds Checking
- Input Validation
- Safe String Functions
- Memory Protection Mechanisms
- Static and Dynamic Analysis
- System Testing

Always be sure to validate input data to verify it does not exceed the allocated buffer size. This is a good way to prevent the easy attacks from occurring since we are checking for it early and often. Then we need to implement strict input validations to filter out unexpected data that could be malicious. For developers working in different programming languages, make sure to check the IDEs for warnings they provide or use the more secure alternative of different functions that appear to do the same thing. In C for example using+ safer string manipulation functions that automatically handle buffer size checks, such as ‘strncpy()‘ instead of ‘strcpy()‘. Additionally, utilizing different code analysis tools during both the development and testing phases to potentially identify buffer overflow (or other related) vulnerabilities. Lastly, everything needs to be tested in many different ways by both developers and testers to try and identify and weak points in the system. This method of intense stress testing of all edge cases will help reduce the chance of bugs and vulnerabilities from being easy to find.

17.2.3 Defensive Programming Techniques

Another concept for incorporating good software development techniques is defensive programming,which can further enhance the security of our software. Some items include:

- Fail-Safe Defaults
- Error Handling
- Security Training
- Secure Coding Guidelines
- Code Reviews

When having choices of items to check for, like a switch statement for example, always use default values or default cases to prevent undefined behavior. This idea can then be extended into implementing proper error handling mechanisms to gracefully handle unexpected situations and prevent system crashes. Or maybe in specific cases force the program to exit or crash depending on the severity of the issue at hand. There are lots of different techniques and strategies available to help with this, which is why it is important to be able to educate developers about common security concerns and solutions. Regular training for all developers will be important to ensure that people are up to par with the thins they should be looking out for. Then we can create and adhere to these established coding standards and best practices to keep consistency and reduce the likelihood of introducing common vulnerabilities. Since developers will always be working in teams, they need to be keep themselves honest, this is done by regular code reviews since it can be easy for a single developer to overlook a fault by accident. Having a team of people checking everything that is added to the repositories will help reduce these bugs and vulnerabilities.

17.2.4 General Best Practices

In addition to to the methods and techniques mentioned earlier, developers should also adopt the following general practices to design overall secure systems:

- Principle of Least Privilege
- Regular Updates and Patching
- Stress Testing

In our programs we want to limit access permissions to the minimum necessary for each user or system component to reduce the potential impact of security breaches. This is because if a system has access to stuff it does not ever use and it is compromised, then the attacker has an easier time getting what they may be looking for. we also want to keep all of our software dependencies, libraries, and frameworks up-to-date with their respective security patches and fixes to address any known issues. Conduct regular stress tests that can act as a threat to identify potential security issues.

By incorporating these practices and principles into the software development process, organizations can significantly reduce the risk of buffer overflows and other common vulnerabilities, ultimately enhancing the overall security posture of their information systems.

Chapter 18

System and Information Integrity

(i) *Identify, report, and correct information and information system flaws in a timely manner;*

(ii) *provide protection from malicious code at appropriate locations within organizational information systems; and*

(iii) *monitor information system security alerts and advisories and take appropriate actions in response.*

Maintaining our systems and information integrity is a crucial aspect to safeguarding our sensitive data that we have. This chapter outlines procedures and protocols to identify, report, and to mitigate flaws in our systems, provide protection against malicious code, and effectively monitor security alerts.

18.1 Information and Systems Flaws

Identifying, reporting, and correcting information and information system flaws in a timely manner is fundamental to maintaining the integrity of our operations. This section details the steps involved in this process:

- Identifying system flaws
- Reporting system flaws
- Correct the flaws

In order for us to identify system flaws we must have regular system audits, vulnerability scans, and user feedback mechanisms. These all serve as important components of our approach to identifying potential flaws in our systems. These measures help in detecting vulnerabilities and weak points. Not only that, they also enable us to address them promptly, ensuring the security and integrity of our systems. By continuously evaluating our systems through these methods, we decrease our chances of encountering risks and maintain a defense against these potential threats.

A reporting channel will be established to facilitate the quick reporting of identified flaws within our information systems. This channel provides employees with a way to securely and confidentially report any threats, vulnerabilities, or any anomalies they encounter while they are using company resources. Employees are encouraged to use this reporting mechanism as part in maintaining the security of our systems. Additionally, regular communication and awareness

is used to reinforce the importance of reporting and to ensure all employees are aware of the reporting procedures.

Once we receive reports of any system flaws, our IT team can quickly initiate a thorough assessment to understand the severity of the reported issues. Once evaluated, appropriate counter-measures such as updates, fix-packs, or system modifications are deployed to address the identified system flaws. This approach ensures that vulnerabilities are mitigated in a timely manner, minimizing any potential risks to our information systems.

18.2 Protection of Malicious Code

Preventing the intrusion or introduction of malicious code is essential to safeguarding our systems and data. This section details the steps involved in this process:

- Implementing robust antivirus software
- Enforcing access controls
- Regular software updates

To accomplish this, all of our systems will have some of the latest antivirus software. This is maintained specifically to detect and remove any malicious code that may threaten the integrity of our data and operations. By prioritizing the integration of up-to-date antivirus software across our infrastructure, we improve our resilience against any malicious code. Additionally, monitoring and analysis of antivirus alerts enable our IT security team to quickly respond to potential threats, minimizing the impact on our systems and maintaining a secure computing environment.

We can also use our access controls to restrict entry to sensitive systems and data. This is a crucial part of our risk mitigation protocols against malicious code. By carefully managing permissions and privileges, we decrease the chances of unauthorized access of critical assets. This measure not only helps prevent malicious actors from gaining foothold within our infrastructure but also enhances our ability to detect and respond to unauthorized activities promptly. Like stated in other chapters, regular reviews and updates of access policies ensure that our security measures remain accurate. Thus, improving our defenses and upholding the confidentiality and integrity of our sensitive information and systems.

Finally, regularly updating software and applications with the latest security patches plays a huge role in improving our defenses against potential threats. These updates are important since they also address known vulnerabilities and weaknesses.

18.3 Monitoring Security Alerts

Careful monitoring of security alerts and advisories is important to stay ahead of potential security threats. This section details the steps involved in this process:

- Utilizing threat intelligence sources
- Establishing an incident response team

Being informed by reputable threat intelligence sources gives us timely and comprehensive information on emerging security threats. By staying ahead of the latest trends and tactics used by security experts, we are better prepared to anticipate and mitigate potential risks to our systems. This approach enables us to adapt our security measures effectively, by implementing any necessary safeguards to defend against evolving threats. In general, utilizing information from these sources allows us to make more informed and accurate decisions so we can allocate resources effectively to strengthen our security.

A dedicated incident response team is an important part in our security framework. By maintaining a specialized team focused on incident response, we can effectively and quickly mobilize resources and expertise to mitigate risks, restore normal operations. Continuous training ensure that our incident response procedures remain agile and responsive to evolving security challenges, increasing our ability to effectively manage and mitigate potential incidents.

Appendix A

Computer Security: Principles and Practice

1. Chapter 3.2, "Password Selection Strategies", page 127 - *"A good technique for choosing a password is to use the first letter of each word of a phrase. However, do not pick a well-known phrase like 'An apple a day keeps the doctor away' (Aaadktda). Instead, pick something like 'My dog's first name is Rex' (MdfniR) or 'My sister Peg is 24 years old' (MsPi24yo). Studies have shown users can generally remember such passwords, but they are not susceptible to password guessing attacks based on commonly used passwords."*

2. Charlie Fripp, "Use this chart to see how long it'll take to crack your passwords" - *" If your password comprises numbers, upper and lowercase letters and symbols, it will take a hacker 34,000 years to crack – if it's 12 characters long."* add link here.