#### 

IT Strategic Solutions – MMT2 Task 1

John Deardurff

Western Governors University

Table of Contents

[A. Perform a SWOT analysis of existing infrastructure 5](#_Toc513442596)

[A1. Strengths 6](#_Toc513442597)

[Employee Experience & Initiative 6](#_Toc513442598)

[Supportive Management 6](#_Toc513442599)

[Fault Tolerant Power 6](#_Toc513442600)

[Site Resiliency 7](#_Toc513442601)

[Server Security 7](#_Toc513442602)

[Improved Monitoring Systems 7](#_Toc513442603)

[Improved Production Reporting 7](#_Toc513442604)

[A2. Weaknesses 8](#_Toc513442605)

[Single Internet Provider 8](#_Toc513442606)

[Wireless Security 8](#_Toc513442607)

[Limited Server Capacity 8](#_Toc513442608)

[Lack of Storage Encryption 8](#_Toc513442609)

[Complicated Permission Levels on Document Storage 9](#_Toc513442610)

[Usage of IMAP for receiving email 9](#_Toc513442611)

[Lack of Anti-Malware solution 10](#_Toc513442612)

[A3. Opportunities 10](#_Toc513442613)

[Folder Redirection to reduce computer backups 10](#_Toc513442614)

[Virtual Desktop Infrastructure (VDI) 10](#_Toc513442615)

[Extend Collaboration on email server to a SharePoint solution. 11](#_Toc513442616)

[Increase Security on Disk and Document Storage 11](#_Toc513442617)

[Upgrade Servers to 64-bit Operating Systems. 11](#_Toc513442618)

[Update Intrusion Detection to Intrusion Prevention 11](#_Toc513442619)

[Take advantage of Cloud-based services 12](#_Toc513442620)

[A4. Threats 12](#_Toc513442621)

[Loss of Internet Services 12](#_Toc513442622)

[Attack against Wireless Devices 12](#_Toc513442623)

[Reduction in Performance 12](#_Toc513442624)

[Spam Relay on Email Server 13](#_Toc513442625)

[Loss of Skilled Staff 13](#_Toc513442626)

[Potential for Ransomware attacks 13](#_Toc513442627)

[B. Analyze SWOT analysis results 13](#_Toc513442628)

[B1. Leverage of Strengths 13](#_Toc513442629)

[B1a. Leverage of Opportunities 14](#_Toc513442630)

[B2. Deficiencies in Threats and Weaknesses 14](#_Toc513442631)

[Deficiencies in Weaknesses - Single Internet Provider 15](#_Toc513442632)

[Deficiencies in Weaknesses – Wireless Security 15](#_Toc513442633)

[Deficiencies in Weaknesses – Limited Server Capacity 15](#_Toc513442634)

[Deficiencies in Weaknesses – Lack of Storage Encryption 15](#_Toc513442635)

[Deficiencies in Weaknesses – Complicated Permission Levels 16](#_Toc513442636)

[Deficiencies in Weaknesses – Using IMAP for Receiving Email 16](#_Toc513442637)

[Deficiencies in Weaknesses – Lack of Ant-Malware Solution 16](#_Toc513442638)

[Deficiencies in Threats – Loss of Internet Services 17](#_Toc513442639)

[Deficiencies in Threats – Attack against Wireless Devices 17](#_Toc513442640)

[Deficiencies in Threats – Reduction in Performance 17](#_Toc513442641)

[Deficiencies in Threats – Spam Relay on Email Server 17](#_Toc513442642)

[Deficiencies in Threats – Loss of Skilled Staff 18](#_Toc513442643)

[Deficiencies in Threats – Potential for Ransomware Attacks 18](#_Toc513442644)

[B3. Deficiency with Greatest Impact 18](#_Toc513442645)

[C. Research Potential Solutions 18](#_Toc513442646)

[C1. Research Strategies 18](#_Toc513442647)

[C1a. Current Technology Examples 19](#_Toc513442648)

[C2. Staying Informed 19](#_Toc513442649)

[C2A. Emerging Technology Examples 20](#_Toc513442650)

[D. Recommendation 20](#_Toc513442651)

[D1. Justification 20](#_Toc513442652)

[E. Sources 21](#_Toc513442653)

# Perform a SWOT analysis of existing infrastructure

|  |  |
| --- | --- |
| ***Strengths***   * Employee Experience & Initiative * Supportive Management * Fault Tolerant Power * Site Resiliency * Server Security * Improved Monitoring Systems * Improved Production Reporting | ***Weaknesses***   * Single Internet Provider * Wireless Security * Limited Server Capacity * Lack of Storage Encryption * Complicated Permission Levels on Document Storage * Usage of IMAP for receiving email * Lack of Anti-Malware solution |
| ***Opportunities***   * Folder Redirection to reduce computer backups * Implement Virtual Desktop Infrastructure (VDI) * Extend Collaboration on email server to a SharePoint solution. * Increase Security on Disk and Document Storage * Upgrade Servers to 64-bit Operating Systems. * Update Intrusion Detection to Intrusion Prevention * Take advantage of Cloud based services | ***Threats***   * Loss of Internet Services * Attack against Wireless Devices * Reduction in Performance * Spam Relay on Email Server * Loss of Skilled Staff * Potential for Ransomware attacks |

## A1. Strengths

### Employee Experience & Initiative

Starting with the Executive Director, Sabelle Arnold, it is apparent that the IT personnel have extensive knowledge and experience. It is not often the Executive of a company has a master’s degree in Information Technology. With over 12 years’ experience in IT Management, it is equally evident that Cameron Kern encourages and supports innovation within the workforce. Firstly, with Sidney Jeffrey who as a data analyst is relied upon to provide data to support business decisions. Taylor Muelles improved machinery efficiency and monetary savings by developing a new system for production reports. The initiative of the employees is clearly shown in Bailey Wynne who not only went back to earn a bachelor’s degree but took the skills to increase the efficiency of the digital monitoring system. The remaining IT staff has all, in their own way, contributed to the overall health of the company by using their knowledge, experience, and innovation.

### Supportive Management

Equally evident in researching this company is that support comes from the Executive Director and flows down through management to the IT Staff. Sabelle Arnold, has a positive comment to make about each employee and the IT Manager, Cameron Kern, constantly and consistently motivates the IT team to acknowledge each person’s achievements.

### Fault Tolerant Power

Each of the locations are equipped to handle power interruptions that could occur for any variety of reasons by using independent transformers, Uninterruptible Power Supplies (UPS), Battery Backups, and a diesel-powered generator.

### Site Resiliency

Each physical site can operate independently by having their own internet connection and servers. It addition, by backing up data to an offsite location the company can ensure resiliency in operations if one site in offline for any length of time. Redundant access points are used to permit service rerouting to alternate paths in the case of network issues. Finally, the database and web servers are duplicated to each location with each site being independently supported by fault tolerant power solutions.

### Server Security

The servers in each location are secured in locked cabinets with restricted access to only a few personnel. The SQL Server and FTP Servers are using SSL encryption to protect data in transit. Additionally, an intrusion detection system is in place to analyze traffic for threats and attacks. Finally, physical security at each location is a high priority for all members of the IT staff.

### Improved Monitoring Systems

Bailey Wynne’s initiative helped improve the efficiency of the high-definition digital monitoring system. Sawyer Molinas worked with the plant staff to develop security monitoring systems that prevent loss due to environment conditions. These improvements in monitoring systems yielded cost savings that can be reallocated to other aspects of the company that could benefit future customers.

### Improved Production Reporting

The system that Taylor Muelles developed for production status reporting has yielded a reduction in energy usage thereby showing monetary savings that can be reallocated to other aspects of the company that could benefit future customers.

## A2. Weaknesses

### Single Internet Provider

The company is using a single tier-one internet service that is providing the capacity and backups for both sites. This leads to a single point of failure if that service provider has an outage. To fix this solution, a secondary internet provider should be obtained.

### Wireless Security

Each wireless connection is using MAC address filtering that does provide a level of security for Wi-Fi access. However, using WPA encryption is enabling false security. A simple Google search will describe instructions to any hacker on attack methods to compromise the wireless access points. A better solution would be to incorporate the 802.1x standard on the wireless access points to force employees to authenticate before gaining access to the network and then using an IPSec solution to encrypt the network traffic.

### Limited Server Capacity

Recently, Ms. Arnold updated the IT infrastructure for a 20% growth of server, storage, and system usage. The proposed update to two new locations will need resources for 100% growth. This weakness could be an opportunity to investigate reducing capital expenditures by looking into a cloud-based server solution.

### Lack of Storage Encryption

Laptops, desktops, and servers will be using a combination of internal and external drive storage. Encryption is not currently being used in any of these devices which could lead to data leakage of confidential company data. This could be solved by using Encryption File Services (EFS) to encrypt individual files and folders. For drive encryption, BitLocker could be used to prevent loss of data, especially in the case of a lost or stolen laptop.

### Complicated Permission Levels on Document Storage

The file and permission structures are overly complicated, outdated, and difficult to manage at the individual employee level. Using a group-based strategy for document security will allow for easier management of permissions, especially as the company continues to grow. Additionally, using newer server operating systems would allow the company to use Dynamic Access Control (DAC) which use a claims-based approach to provide access based off attributes and claim rules. An additional solution to control document security would be using an Information Right Management (IRM) system to control specific right to documents.

### Usage of IMAP for receiving email

Using IMAP on email systems leads to needing to provide an SMTP relay solution on your email servers. If not configured correctly this could lead to the email server being used as a spam server for anyone with a basic knowledge of SMTP commands. Additionally, by turning off the IMAP protocol, the company would be able to close both ports 143 and 993 on their firewalls. I would also suggest identifying if the email server has the POP3 service running and turn it off as well, thereby being able to close ports 110 and 995 on the firewalls. SMTP should be used for both sending and receiving email.

### Lack of Anti-Malware solution

While the company is using anti-virus solutions on portions of the network. There was not an anti-Malware solution mentioned in the documentation. This would lead to possibly being susceptible to malicious attacks, most notably ransomware attacks that have become more popular of the last few years.

## A3. Opportunities

### Folder Redirection to reduce computer backups

Currently, all computers in the network are being backed up. By implementing a Group Policy to perform Folder Redirection, any user files that are stored locally to network computers will be redirected to the file server. This will reduce network traffic and time needed for backups. This would also increase the management of client machines by being able to re-image computers without worrying about data loss.

### Virtual Desktop Infrastructure (VDI)

The company is currently distributing applications from an application server to each computer to reduce needing to image computers and install software. This could be taken one step further by incorporating virtualization technology like Hyper-V or VMware to allow users to connect to virtualized desktops hosted on centralized servers. Single images can be created and shared with multiple users who need similar applications. This reduces capital expenditures of client desktops, increases the types of devices supported, and reduces management of user devices. In addition, data is more secure as it is protected in the server room.

### Extend Collaboration on email server to a SharePoint solution.

Currently, the email server is being used not only for email, but as an entire collaboration solution. An opportunity could be taken to move shared calendaring, contacts, tasks, and events to a SharePoint server that would provide a centralized web-based solution for all employees.

### Increase Security on Disk and Document Storage

An opportunity could be taken to redesign the security structure of both the disk and document storage by incorporating encryption technologies such as EFS and BitLocker, as well as, updating rights and permissions through Dynamic Access Control and/or an Information Rights Management server.

### Upgrade Servers to 64-bit Operating Systems.

It was mentioned that the file server is currently running on a 32-bit OS. Microsoft Server 2012 R2 and later require 64-bit processors. During the upgrade process, it would be an excellent opportunity to identify servers that need to move to a 64-bit architecture and operating system.

### Update Intrusion Detection to Intrusion Prevention

Many of the security systems in place are using automation to proactively monitor and control access to the network. The exception to this is the intrusion detection system. By taking the opportunity to upgrade to an intrusion prevention system, this would extend out the automation of proactively secure the network infrastructure.

### Take advantage of Cloud-based services

As the company is expanding and looking to purchase additional servers, this would be a great opportunity to investigate cloud-based services such as Microsoft Azure or Amazon Web Services. Using a cloud-based solution could reduce staff needed to manage the corporate network, reduce the capital and operational expenses, and provide more agility and elasticity to future growth.

## A4. Threats

### Loss of Internet Services

There is a single point of failure as the company is using a single tier-one internet service that is providing the capacity and backups for both sites. A secondary internet provider should be obtained to fix this solution.

### Attack against Wireless Devices

Using WPA encryption leaves the wireless access points susceptible to attacks. A solution to solve this issue would be to incorporate the 802.1x standard on the wireless access points to force employees to authenticate before access the network and then use an IPSec solution to encrypt the network traffic.

### Reduction in Performance

Currently the IT infrastructure will only allow for a 20% growth. Expansion without planning for the 100% growth to the additional locations would reduce the performance of the current infrastructure.

### Spam Relay on Email Server

Having IMAP and possibly POP3 protocols open on the email server leaves the environment susceptible to become a spam relay server if not properly secured and configured. The best practice is to identify if these protocols are still in use and remove them from the email servers.

### Loss of Skilled Staff

As previously mentioned, one of the biggest strengths the company has is the experience and innovation of the IT staff. Loss of these skilled staff members could lead to institutional knowledge loss and possible morale strain. To mitigate this threat, staff retention should be a primary goal as part of IT planning.

### Potential for Ransomware attacks

Without an anti-malware strategy, the company leaves itself open to possible ransomware attacks or potential data loss. It is important to implement anti-malware software into the network.

# Analyze SWOT analysis results

## B1. Leverage of Strengths

IT Infrastructure is comprised of all the resources needed to provide technology support for a company. This includes tangible investments like hardware equipment, software applications, and data storage. But also included in the IT infrastructure is the personnel needed to manage the network environment. Three strengths that can be leveraged to improve the company’s existing services is encapsulated in the initiative and innovation of the IT staff. The system that Taylor Muelles developed for production status reporting has yielded a reduction in energy usage. Bailey Wynne’s initiative helped improve the efficiency of the high-definition digital monitoring system. Sawyer Molinas worked with the plant staff to develop security monitoring systems that prevent loss due to environment conditions. The experience of the IT personnel, the improvements to the production status reporting system, and the improvements in the monitoring systems are three strengths that have been used to realize monetary savings that can be reallocated to other aspects of the company that could benefit both new and future customers.

## B1a. Leverage of Opportunities

Three opportunities that could be leveraged within the current infrastructure to bring new products or services into the marketplace would be investigating cloud-based services for server expansion, implementing SharePoint to extend collaboration, and implementing an Information Rights Management system to secure customer information. Investigating cloud-based services will allow the ability to provide agility and elasticity to the company’s servers. This would allow the company to be able to quickly expand into newer markets much quicker if future expansion is needed. SharePoint could be used on-premises or as a cloud-based platform to provide collaboration not only with employees, but also with new vendors and customers. Finally, by increasing security for disk and document storage with an Information Rights Management system, data leakage would be prevented, and it would increase customer confidence in both the old and new products and services of the company.

## B2. Deficiencies in Threats and Weaknesses

The deficiencies in threats and weaknesses in the current IT infrastructure basically comes down to availability and security.

### Deficiencies in Weaknesses - Single Internet Provider

The loss of internet services by only having a single internet provider could reduce the availability of services to both employees and customers. Thus, resulting in downtime and lost productivity of employees or loss of customer contact during the service unavailability.

### Deficiencies in Weaknesses – Wireless Security

Using WPA encryption is enabling false security. While users assume that using WPA encryption makes them safe, a simple internet search will describe instructions to any hacker on attack methods to compromise the wireless access points. A better solution would be to incorporate the 802.1x standard on the wireless access points to force employees to authenticate before gaining access to the network and then using an IPSec solution to encrypt the network traffic.

### Deficiencies in Weaknesses – Limited Server Capacity

Limited server capacity could lead to slow access or availability to those same services if expansion is not planned for future growth. Ms. Arnold has only allowed for a 20% growth, while the planned upgrade will be a 100% growth.

### Deficiencies in Weaknesses – Lack of Storage Encryption

Encryption is not currently being used in any of these devices which could lead to data leakage of confidential company data. This could be solved by using Encryption File Services (EFS) to encrypt individual files and folders. In addition, since laptops, desktops, and servers will be using a combination of internal and external drive storage, A drive encryption technology like BitLocker should be used to prevent loss of data, especially in the case of a lost or stolen laptop.

### Deficiencies in Weaknesses – Complicated Permission Levels

The file and permission structures are currently being managed at the individual employee level which is overly complicated, outdated, and difficult to manage. Easier permission management for document security would be to use a group-based strategy, especially as the company continues to grow. Additionally, using newer server operating systems would allow the company to use Dynamic Access Control (DAC) which use a claims-based approach to provide access based off attributes and claim rules. An additional solution to control document security would be using an Information Right Management (IRM) system to control specific right to documents.

### Deficiencies in Weaknesses – Using IMAP for Receiving Email

Using IMAP on email systems will lead to the email being compromised and being used as a spam server which would lead to loss of customer trust, degradation of server performance, and the possibility of having the company email address blocked by much of the internet. It is recommended that IMAP and POP3 protocols be turned off and only SMTP should be used for both sending and receiving email.

### Deficiencies in Weaknesses – Lack of Ant-Malware Solution

Over the last few years, ransomware attacks have been on the rise. To prevent the company from being susceptible to malicious attacks on their network an anti-Malware solution should be implemented.

### Deficiencies in Threats – Loss of Internet Services

The company is currently using a single tier-one internet service that is providing the capacity and backups for both sites. A secondary provider should be obtained to prevent a single point of failure in internet services.

### Deficiencies in Threats – Attack against Wireless Devices

Using WPA encryption leaves the wireless access points susceptible to attacks. A solution to solve this issue would be to incorporate the 802.1x standard on the wireless access points to force employees to authenticate before access the network and then use an IPSec solution to encrypt the network traffic.

### Deficiencies in Threats – Reduction in Performance

The company is planning for a 100% growth with the addition of two new locations. The IT infrastructure is only allowing for a 20% growth. Additional planning needs to be incorporated to ensure that the network will be able to handle this growth without causing performance issues or the lack of availability to services.

### Deficiencies in Threats – Spam Relay on Email Server

Having IMAP and possibly POP3 protocols open on the email server leaves the environment susceptible to become a spam relay server if not properly secured and configured. The best practice is to identify if these protocols are still in use and remove them from the email servers.

### Deficiencies in Threats – Loss of Skilled Staff

One of the biggest strengths the company is the innovation and experience of the IT staff. Loss of these skilled staff members could lead to institutional knowledge loss and possible morale strain. To mitigate this threat, staff retention should be a primary goal as part of IT planning.

### Deficiencies in Threats – Potential for Ransomware Attacks

The company has left itself open to possible ransomware attacks or potential data loss by not having an anti-Malware solution in place. It is important to implement anti-malware software into the network to prevent data loss or data leakage.

## B3. Deficiency with Greatest Impact

The deficiency with the greatest impact is the several security issues observed in the IT infrastructure, primarily the lack of storage encryption. With the company using external storage the leakage of data is highly probable with the loss or theft of any external storage device. Additionally, as more people are using laptops, tablets, and other mobile devices it is more prevalent that those devices get lost or stolen. By using both Encryption Files Services (EFS), BitLocker for Drive Encryption, and the addition of an IRM solution. This deficiency in security could be combated and reduced.

# Research Potential Solutions

## C1. Research Strategies

As a Microsoft Certified Trainer (MCT) it is literally my job to stay up to date with both current and emerging technologies. Just yesterday, I taught a class on Active Directory Rights Management Services (ADRMS) which has the Information Rights Management (IRM) solution built into Windows since Server 2008. In addition, I also teach a class on Encryption File Services (EFS) and BitLocker for Drive Encryption. EFS has been a part of the NTFS file system that has been included in Windows since the late 1990’s. That same course includes BitLocker for Drive Encryption that was introduced with Windows XP and Windows Server 2003. However, I should not only rely on my own knowledge when researching technologies. I also used <http://docs.microsoft.com> which is Microsoft’s main website for all their documentation. For this article, I started with the Encryption Overview article. (Neira, B. , August 08, 2017). For further research, I would use Google to search for encryption technologies for non-Microsoft environments.

## C1a. Current Technology Examples

Two current technologies that should be used to combat and reduce the deficiency in storage encryption is Encryption Files Services (EFS) for individual files and folders and BitLocker to encrypt physical hard drives. Additionally, I would recommend an Information Rights Management (IRM) solution to add additional rights and permissions to documents.

## C2. Staying Informed

A strategy to stay informed with current and emerging technologies would be to continue to subscribe to online magazines, vendor email lists, reviewing videos from online conferences, attending conferences and weekend events. I’ve been in the IT industry for over 25 years and teaching IT for the last 20 years. I spend at least 4-5 hours everyday researching current and emerging technologies.

## C2A. Emerging Technology Examples

Two emerging technologies that would help the company gain a competitive advantage would be Azure Cosmos DB (Azure Cosmos DB Documentation, May 5, 2018) and Containers (What is a Container, December 12, 2017).

Azure Cosmos DB is a NoSQL solution that could be used as a document store for a more efficient and secure environment. Cosmos DB has comprehensive service level agreements to ensure throughput, availability, and consistency guarantees. Containers could be used to create smaller stand-alone executable packages for their custom applications. Containers are based on open standards that can run on all major operating systems and act as a way of isolating application from each other making them more secure.

# Recommendation

If selecting just a single recommendation for the company I would suggest using the Encryption File System (EFS) to secure all of their documents and data.

## D1. Justification

The reason I would suggest EFS is because it is a built-in file encryption tool for the Windows file systems. EFS enables transparent encryption of files and a person that does not have the correct key cannot read the encrypted data. Even if someone gains physical possession of a computer or external drive, encrypted files will keep the data protected. If choosing additional components of a defensive strategy, a further recommendation should be to use additional applications such as BitLocker for Drive Encryption and an Information Right Management (IRM) solution.

# Sources

Neira, B. (2017, August 08). Encryption overview. Retrieved May 5, 2018, from <https://docs.microsoft.com/en-us/azure/security/security-azure-encryption-overview>

Azure Cosmos DB Documentation - Tutorials, API Reference. (n.d.). Retrieved May 5, 2018, from <https://docs.microsoft.com/en-us/azure/cosmos-db/>

What is a Container. (2017, December 12). Retrieved from <https://www.docker.com/what-container>