**Secure Network Design**

Western Governors University

December 26, 2023

**A: Business Requirements**

In preparing for this merger there are important factors to take into consideration. Based upon the current business requirements, the merger will introduce new risks to network security and infrastructure for both companies.

While evaluating company A, it is important to note that they are a global company. Since company A is operating on a global scale, they must take into consideration compliance and regulations in each country that they are doing business in. If they mishandle consumer data, they could be subject to fines. They are acquiring a company which provides software to medical companies and collects credit card information as a payment option. This increases the attack surface of company A substantially. Fortunately, there are methods to mitigate this risk which will be covered in depth in this report.

See below for a summarization of the Network Security and Infrastructure problems for company A and company B.

**Network Security Issues**

Company A

* Collection of credit card information increases risk exposure.
* Global presence increases attack surface and potential for fines from compliance issues.

Company B

* Currently relies on a third-party vendor for infrastructure support. If this vendor is compromised it could compromise company Bs data.
* Company B has been operating their business without a Cyber Security professional, it is likely that they have not implemented a defense in depth strategy. This is a requirement given the sensitivity of the data they are handling.

**Infrastructure Issues**

Company A

* Usage of older systems which don’t allow for scalability.
* Usage of older systems which don’t allow for redundancy.

Company B

* Infrastructure is managed by a third party.
* Currently not using zero trust principles.

**B1: Vulnerabilities**

In reviewing company B’s vulnerability scan, there were two very severe vulnerabilities noted:

* Company A has vulnerabilities in the implementation of the Ruby code using DRb.
* MFA has not been enforced across all users.

In reviewing company A’s vulnerability scan, there were two very severe vulnerabilities noted:

* Company B has open ports 21-90 and 3389.
* User accounts no longer required are not removed.

**B2: Impact, Risk, and Likelihood**

Company B has vulnerabilities in its implementation of the Ruby code using DRb. A malicious actor can potentially exploit the vulnerabilities in the code and achieve remote code execution. Since company B is a global financial company, this vulnerability is a serious threat. If a malicious actor can achieve remote code execution, they can gain access to compromised devices and potentially view and even manipulate sensitive data. Since the vulnerability scan mentioned this code vulnerability is highly critical, this indicates that there is a high likelihood that this can be exploited. Company B provides checking accounts and investment products, if these accounts are compromised this can result in financial loss. In addition to asset loss, and reputation damage, the company may also receive large fines for lack of compliance. This should be remediated asap.

Company B does not have Multifactor Authentication across all accounts. This is a serious risk as some of the passwords only require 8 digits. With the right software or reconnaissance tactics a malicious actor could potentially gain access to a user’s account by cracking their single password. Multifactor would require would make it more challenging for a malicious actor to gain access, even if they figured out a user’s password they would still be required to authenticate via specified device or alternative method. This is a moderate risk as a compromised account may have access to sensitive documents and customer PII. A malicious actor could also send phishing emails to employees within the company using the compromised account. This would allow the attacker to move laterally throughout the organization. There is a high likelihood of this happening as the company could be considered a target for sensitive data that they deal with. If employees are only using single factor authentication with 8-digit passwords the chances of this event happening increases.

Company A has open ports: 21-90, 3389. Having these ports open increases the attack surface and provides potential access points for malicious actors. Port 3389 is associated with remote access. If an attacker gains access to port 3389 they can gain control of devices that have RDP enabled. This is a severe risk because it allows an attacker entry points into systems. Company A provides specialized software to medical providers. Since medical providers have been at risk of ransomware, company A could be a target for malicious actors. To avoid systems being compromised company A should only use secure ports, in addition that could close ports that are not in use.

Company A is not deactivating accounts that are no longer required. This is a serious risk that can be created from insider threat. Disgruntled employees might maintain access to sensitive systems even after they leave. Malicious actors can also attempt to gain access to these idle accounts to access sensitive information. Because of the nature of the industry that company A specializes in, it is important to remediate this as soon as possible.

**C: Topology Diagram**

Figure 1  
*Company A*

A diagram of a computer network

Description automatically generated

Figure 2

*Company B*  
A diagram of a computer network

Description automatically generated

Figure 3  
*Azure Cloud*

A cloud with blue doors

Description automatically generated

**D: Topology Components**

|  |  |  |
| --- | --- | --- |
| **Device** | **OSI Layer** | **TCP Layer** |
| Firewall (Cisco and Sophos) | Network Layer | Network Layer |
| Router (Cisco) | Network Layer | Network Layer |
| Servers (moved to Azure VMs) | Data Link  Layer | Network Access  Layer |
| Cabling (cat6a and cat5e) | Physical Layer | Network Access Layer |
| VPN (VPN Gateway) | Network Layer | Network Layer |
| Laptops and Workstations | Application Layer | Application Layer |

**E: Rationale**

There were many components that were added, deleted, and repurposed in the newly merged topology diagram. These changes were completed to increase security, decrease attack surface, mitigate risk, and increase potential for scalability across the network.

For company A the physical servers were moved to VM servers on Azure. These servers consisted of: Exchange Server, File Server, Application Server, and SharePoint Server. Moving these to the cloud will create resources to be utilized more efficiently as they can scale based upon demand. This will reduce resources that are required to safeguard these sensitive servers such as physical rooms and surveillance. The attack surface will be minimized, as disgruntled employees with physical access to the room will no longer be able to compromise the system or steal data. Accessibility will now be allocated based on limited granted user access using the principle of least privilege and separation of duties. Moving these components to the cloud creates more flexibility as the VMs will be able adjust specifications to meet their specific needs. This will also increase data availability through means of redundancy. In the event of hardware failure traffic will be redirected increasing uptime. Using the cloud for the servers will also reduce the costs of physically maintaining servers, this would include repairs, replacements, and upgrades. The transition to the cloud will also help to ensure compliance with industry standards. Compliance with the industry standards will help to avoid hefty fines as the company continues to scale upwards. I will explain compliance more in depth in Section G. Prior to the merger and network update, Company B was relying on a third party for infrastructure needs. We have decided to remove this third party and share redundant servers on the cloud. This will free up capital by removing the current subscription and splitting costs of cloud management. In addition, it allows us to tighten up security by removing a point of failure and have more centralized control and awareness.

Remote access to workstations and computers from the public internet was a serious threat to security. If a malicious actor were able to gain remote access, they would be able to alter, steal, or leak data. Because of the sensitivity of the information that both companies possess we altered the systems so that remote access can only be gained directly through the cloud. We now use VPN gateways to establish secure encrypted connections. This greatly reduces a serious threat to sensitive data. In addition, only a handful of IT specialists with granted access will be allowed to have remote control upon request. If an employee with this access leaves the company their account and access will be removed instantly.

Network segmentation was applied to both company A and B. For these companies we separated the Workstations from the laptops. The reason for doing this is to reduce the risk of malicious actors moving laterally should they compromise a system. This makes it easier to isolate and contain events. For example, if a malicious actor were able to gain access to the wireless network through a vulnerability the threat would be mainly limited to devices connected to that network. This reduces the attack surface and helps to safeguard sensitive data. This is also useful as laptops are mobile and can potentially be used on other mobile networks, and they can be lost or stolen. The added vulnerability in using mobile devices makes laptops more susceptible to being compromised.

In both networks firewalls were added in between the ISP and the DMZ, then in between Laptop/Workstations and the DMZ. This setup allows us to filter out unwanted traffic. This adds an extra layer of defense making it more difficult to penetrate workstations/laptops. These components and network structure will allow us to control traffic flow, create access control lists, and further isolate areas of the network for added safety.

We noticed company B had two wireless access points. One of which is dedicated to a guest network. We moved this guest wireless connection outside of the internal network as it posed a risk in its previous location. We want to ensure that malicious actors cannot move laterally within our network by exploiting vulnerabilities from the guest network.

**F: Secure Network Principles**

By making these modifications to the topology of the network diagrams, I was able to achieve many secure network design principles. The two principles, which are prominent in my design, were: Zero Trust and Principle of Least Privilege.

**Zero Trust**

Moving physical servers to the cloud will create an environment based on user verification and authentication. To access different resources users will need to be authorized. The previous setup was to trust that employees will not access servers on premises and steal/leak sensitive data. We can also easily edit the requirements on the cloud to require MFA and strong passwords for account access. This centralized control allows us to update security controls as necessary in a timely fashion. VPN gateway to the cloud means users accessing the cloud will be doing so on a secured encrypted connection. We are making it very challenging for employees to make mistakes.

By segmenting the laptops and workstations into different parts of the network, we are aligning with the zero-trust model. With the new model, if a user’s laptop is compromised or lost, this incident would be easier to isolate and contain without putting the entire network at risk. Mobile devices are more vulnerable as they access different networks and have the potential to be lost.

Removing the guest Wi-Fi from the internal network removes untrusted devices from the network. Only employees should have that access.

Structuring the firewalls between ISP, DMZ, and Workstations reinforces zero trust by controlling the flow of traffic throughout the network. This will allow us to create access control lists and filter out unnecessary Ips.

Requiring VPN gateways for cloud access and remote access heavily aligns with the principle of zero trust. One of the greatest vulnerabilities I noted in reviewing the scan was the ability to gain remote access via the public internet. If a malicious actor was able to gain control, they would have access to devices sensitive information and could really do serious damage. The VPN Gateway makes it a requirement to have a secure encrypted verified connection.

**Principle of Least Privilege**

In moving to the cloud, users will be granted specific privileges based upon their roles within the company. We removed the physical servers from on premise, so the only way to gain access to specific data will be through the cloud. Users will only be able to access data that is relevant to their work so this will greatly mitigate risk. In addition, when employees change roles or leave the company, it will be easy to assign new privileges or completely remove their account and access.

The network segmentation I applied through the topology will also make it easier to assign privilege based upon the segment that the individual works within, we can identify which devices belong to certain segments.

The firewall positioning also allows us to control the flow of traffic and communication. We can determine which zones communicate within one another to reduce risk.

The VPN gateways are an important component in implementing the principles of least privilege. This is one of the most important as we are determining who will have VPN access based on their roles. The ability to access devices remotely will be very limited.

**G: Regulatory Compliance**

One of the benefits of the proposed merged network topology diagram is that the two companies will become more compliant with regulatory requirements. Because of the unique nature of the industries that businesses operate in, there are a variety of regulations that they must comply with. The regulatory compliance requirements that were most critical are: GLBA and HIPAA.

Company A provides a wide range of financial products: checking accounts, bank cards, and investment products. Because of this, they must comply with GLBA (Gramm Leach Biley Act). It is very important that they protect their customers’ financial information, which is nonpublic. This could include: bank statements, account balances, create card information, social security numbers, physical addresses, and much more. If a malicious actor gained access to this information, it could be very detrimental.

The proposed network topology addresses this regulatory compliance in various ways. By segmenting the networks, introducing firewalls, creating access control lists, and using VPN gateways we are able secure customers NPII and remain compliant with GLBA (Federal Trade Commission, 2022). The remaining compliant will not only protect the customers and employees, but it will also protect the company from large fines. In addition to fines if the company leaks sensitive information their reputation can also be damaged. The principle of least privilege will ensure that only necessary authorized users will have access to sensitive information. The encryption of data also adds another layer of defense.

HIPAA is relevant to companies that deal with PHI. Company B provides software to medical providers. This could entail dealing with medical records which have highly sensitive information. Compliance with HIPAA ensures that companies handling PHI keep the information secure and private. The updated topology significantly reduces the chance of the company’s being fined for mishandling data.

The placement of the firewalls and network segmentation helps to isolate devices which contain PHI and information related to medical providers. Restructuring the network and creating a secure coding policy helps to safeguard this sensitive information. As mentioned earlier in this briefing, company B had vulnerabilities in their Ruby code which can lead to malicious actors gaining remote access.

There were also SIEM tools added to both companies’ network for auditing and logging data. This will allow us to monitor and alert any suspicious activity. This will allow us to extinguish threats before they escalate, and to remain compliant with HIPAA and avoid fines.

**H: Emerging Threats**

While this new network topology implements defense in depth and adds new layers of security, this does not mean that the network is entirely safe from threats. Malicious actors are always coming up with new ways to infiltrate systems.

There are two emerging threats which pose risk to the merged network: Cloud-Based and Zero Day Attacks. Both threats present risk to the network’s security and performance.

In migrating to the cloud, new threats become present. If the cloud is not properly configured this can create a vulnerability to the data. In addition, if Microsoft Azure is breached, then the data stored on the cloud can be accessed. Users will also have access to the data if a malicious actor gains access to an admin account they would have access to information. Performance of important systems can be impacted if Azure network goes down. The largest issue in having servers on the cloud is reliance on the cloud provider.

These potential risks can be easily managed if the proper steps are taken. Regarding configurations, there will be policies in play which require auditing the setup in Azure. User Access will not be a major concern as this was addressed in the defense in depth strategy. Password complexity and multifactor authentication is a requirement which will reduce account compromise. The companies cannot control whether Azure gets breached, however they can make sure that their data is encrypted. This will ensure that even if data is stolen it is hard to interpret.

The second emerging threat is Zero Day Attacks. This takes place when malicious actors target unknown vulnerabilities. As technology advances these are becoming more common. Hackers are constantly searching for new ways to exploit systems. These attacks can be used to steal data or potentially drain a company’s resources. This can be a major concern for a network which is switching to the cloud. Azure can charge users based upon resource consumption. If Malicious actors can perform a DDOS attack it can end up being very costly. A DDOS attack could also slow down the network.

Many of the changes to the topology will help to protect against a Zero Day attack on premises. The firewalls and network segmentation will help to isolate the events if they occur and keep unwanted traffic out. VPN Gateways and data encryption will also help to guard against zero day. The companies will also practice patch management and regular updates, so the software is secure. Moving the servers to the cloud will make it easy to update patches on the cloud on a regular basis.

**I: Summary Recommendations**

When company A and B merge there are going to be many security implications to take into consideration. The vulnerability scans and network diagrams that I was provided indicated that there were critical vulnerabilities in both systems. In addition, the merging of the two companies creates new vulnerabilities. There is a new risk in migrating servers to the cloud, however for these companies, the benefits will greatly exceed the costs.

Before I created the proposed network topologies, I had to properly assess the companies’ financial constraints in addition to the current security posture. I was provided with a budget of $50,000 and I was able to create a new system, which is much more secure for $45,318. I wanted to ensure the on-premise systems were secure before merging on the cloud because of the highly sensitive data that both companies possess. Fortunately, both companies already had some great components which just needed to be repurposed, rearranged, or removed. For the on-premise networks, we purchased three firewalls which totaled $3000, and 4 VPN Gateways which totaled $1248.

The two networks combined have over 200 devices. The current on premise setups made servers with highly sensitive data far too accessible. There was an extreme threat both internally and externally. Neither company was compliant with regulations, leaving them at risk of being fined. If company A receives a fine for not complying with GLBA, as a global financial product company, they could be fined $100,000. If company B is fined for not protecting consumer PHI under HIPAA it could also cost up to $100,000 (U.S. Department of Health & Human Services, 2021).

By switching to the cloud both companies will be able to centrally control user accessibility across the network and mitigate risk. It also removes the need for physical safeguards needed to protect the servers. If the companies decided to maintain on premise systems, I would have recommended biometric access to trusted individuals, for accessibility to a secure room as one of my safeguards to prevent intrusion by insiders. This system alone and set up alone would have exceeded the company’s initial budget.

The risk associated with switching to the cloud is that the companies become dependent on a third party. The recurring fees are subject to change. While it becomes much easier to scale with cloud solutions, if the company begins to grow even larger, they become at the mercy of the cloud provider. In addition, cloud providers are still susceptible to becoming compromised.

Overall, the current probability of encrypted data on the cloud being transferred through VPN Gateways being corrupted or stolen is small, in comparison to the risk of data at rest on premise with over 200 employees with ease of access. If the companies decide to forego the cloud, I highly recommend they invest in offsite data centers, or a private cloud of some sort. This would require increasing the current budget and making a much larger investment. Transitioning to the cloud will be a cost-effective route for both companies to manage data access, remote device access, software/OS updates, and resources.

**References**

Federal Trade Commission. (2022). *Gramm-Leach-Bliley Act*. Federal Trade Commission.   
 https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

US Department of Human Health and Services. (2021). HIPAA for Professionals.   
 https://www.hhs.gov/hipaa/for-professionals/index.html