Network Merger and Implementation Plan

Alhouseny Camara

Department of Information Technology, Western Governors University

Secure Network Design-D482

Professor Bob Curtis

Abstract

As the cybersecurity professional for Company A, I have been assigned to address the security issues and challenges involved in merging the networks of Company B following its acquisition. To ensure that Company B's infrastructure can integrate with Company A's existing infrastructure. Risk-based decisions will be involved for a smooth transition, utilizing the vulnerability scans, network diagrams, and assessments from Company B, comparing them with Company A's risk analysis and network diagram to develop a secure network design to merge the two networks successfully. In the implementation of security designs addressing cloud capabilities/adoption, ensuring compliance, and also budget constraints will need to be taken into account. This paper will give company executives a possible solution to implement the merger.

Requirement A

Based on the business requirements given in this scenario companies A and B both have network security and infrastructure problems that need to be addressed before implementing an assessment on the best approach to merge them.

Company A's Network Security Issue #1

Company A wants to include the use of the Zero Trust Principle in the new security design network showing that their current network structure is based on an outdated model that could be perimeter-based. A perimeter-based network is a security issue because it just focuses on the network boundaries, meaning keeping any external threat from the network out and not paying much attention to the internal traffic, which isn't sufficient anymore. With the acceleration of technology and employees having access to so many devices on the premises, it's important to focus internally on the traffic of the network especially for a global financial company. With the addition of cloud services/capabilities and allowing remote access, the implementation of the Zero Trust Principle will be crucial in securing the network, since it operates on the "never trust, always verify" principle, it will continuously require authentication, authorization, and accounting for each device on the network. By implementing the Zero Trust Principle, Company A's network security will be protected internally and externally against threats and prepared for the upcoming merger with Company B.

Company A's Network Security Issue #2

Company B offers special software to medical providers, meaning that they have to comply with certain regulatory requirements such as HIPAA. This federal law protects the privacy and security of health information. This would be a network issue for Company A since they operate in the financial sector. This regulatory requirement would be something that

wouldn’t necessarily have to be complied with, but with the upcoming merger, it’s now a security issue that must be addressed and implemented into the new security designs.

Company A’s Infrastructure Issue #1

The interest in implementing cloud capabilities to the new network design, and also the interest presented by the executives in wanting to integrate the use of cloud for scalability and redundancy shows that the current infrastructure structure is fully on-premised. The implementation of cloud services will allow the company's IT environment to be more dynamic and efficient.

Company A’s Infrastructure Issue #2

There will be some integration issues since Company B has no dedicated cybersecurity professional role and utilizes third-party support for infrastructure needs. Company B also has similar capabilities and tools to Company A. Company A will need to add or remove similar tools from their IT environment, and if not implemented correctly it can affect the operations and the resource management of Company A.

Company B’s Network Security Issue #1

Company B's lack of dedicated cybersecurity professionals is a network security issue because it leaves the company with its valuable assets vulnerable to attack from threat actors. Cybersecurity professionals would be accountable for implementing network security measures such as Identity and Access Management, and monitoring network traffic. Cybersecurity professionals are the first line of defense in case of a threat actor's exploits. They are also the ones to do vulnerability assessments periodically to ensure compliance and security of the network.

Company B's Network Security Issue #2

Company B accepting credit cards as a payment option without having dedicated cybersecurity professionals can be a network security issue because a potential breach would put customer data at risk. With accepting card payment comes the Payment Card Industry compliance, there will be some requirements such as encryption of data, and network segmentation to further protect customer data, and without having dedicated cybersecurity professionals to apply these leave your company is at risk.

Company B's Infrastructure Issue #1

Company B's total dependence on third-party support is a major potential infrastructure security issue because it creates an over-reliance and trust that threat actors could easily exploit. If third–party support is breached, that directly affects Company B's IT environment and exposes valuable assets that could be used to exploit Company B. Utilizing third-party support also dictates the structure of the infrastructure, which can limit the direct control of what system or resource underlies the core infrastructure of their IT environment.

Company B's Infrastructure Issue #2

As stated previously Company B's over-reliance on third-party support and being a small company can affect how it merges with Company A global infrastructure. Meaning Company B's current infrastructure may not be able to handle the scalability necessary to handle the traffic that comes with Company A. This may lead to integration and performance issues that will need to be addressed before the new security design implementation.

Requirement B

On analysis of the network diagram and the vulnerability scan for both companies, some vulnerabilities need to be addressed that could potentially impact the implementation of the new security design of the merged companies.

Company A vulnerability #1

Company A has multiple open ports that range from 21-90 and also 3389, which are all major potential security vulnerabilities. “Ports enable data packets, consisting of control information and user data, to be communicated throughout a network”(Chow,2021). Understanding the importance of ports shows how leaving them open can lead to vulnerabilities being exploited. Utilizing open ports, threat actors can “identify the different services running, protocols used, and baseline traffic to pinpoint vulnerabilities they can exploit”(Chow, 2021). Threat actors can use this to perform attacks such as man-in-the-middle, where the threat actor changes the communication path between two devices and makes them believe they are directly in communication with each other. Company A also wants to allow remote access to their employees and have port 3389 as an open port, which is giving an open invitation for threat actors to exploit the company since “RDP has a history of security vulnerabilities. Exploitable weaknesses in the protocol itself have been discovered over time, allowing attackers to execute various attacks, ranging from unauthorized access to the compromise of the entire system”(Villanueva, 2024). Securing and closing ports will be essential in the new security design implementation.

- Impact: High

    - This can affect the brand and the reputation of Company A, especially since it is a global financial company.
- Risk: High
    - This is categorized as high because it can give access to multiple systems in the network.
- Likelihood: High
    - This is categorized as high because these ports are well-known to attackers and are often targeted.

Company A vulnerability #2

The fact A all users use eight-character passwords is a vulnerability that needs to be addressed because it allows threat actors to use multiple attacks to breach the company. “According to a recent report published by cybersecurity firm Hive Systems, even 8-character passwords could be cracked quickly. An 8-character password that consists only of numbers or lower-case letters could be cracked instantly, and if the password contained a mix of upper- and lower-case letters, it would only take around 2 minutes to correctly guess”(Anderson, 2022). So it’s not sufficient to have eight-character passwords because they are weak and threat actors only need to crack the passwords of one user and could get access to all the systems in the network, which is a risk a global financial company should not be taking.

- Impact: High
    - This is categorized as high because it can lead to access to unauthorized accounts that could have access to customer data.
- Risk: High

    - This is categorized as high because the attack surface of a threat actor becomes larger since all users have eight-character passwords.
- Likelihood: High
    - This is categorized as high because threat actors use common tactics such as brute force, which “can crack an eight-character password in less than one hour, according to Hive Systems”(Staff, 2023).

Company B vulnerability #1

Company B has a Distributed Ruby (dRuby/RDb) Multiple Remote Code Execution vulnerability, which would allow attackers to “run arbitrary code on a remote machine, connecting to it over public or private networks”(Imperva, 2023). This can lead to system compromise because “RCEs are possibly the most severe type of ACE, because they can be exploited even if an attacker has no prior access to the system or device”(Imperva, 2023). Which could lead to the operations of Company B being affected.

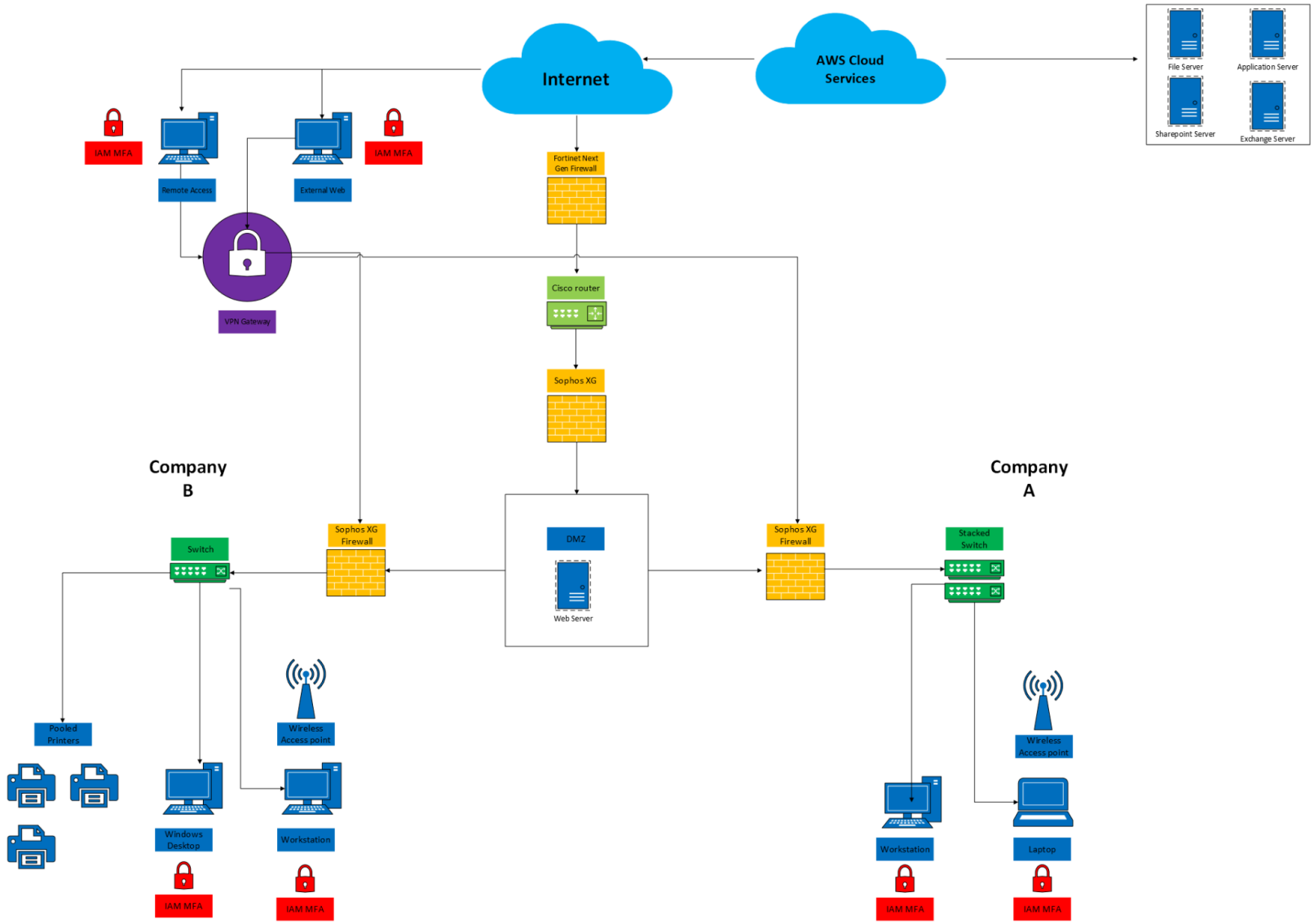
- Impact: High
    - This is categorized as high because if exploited could lead to major exposure of data and sensitive information that a company that handles medical data could not afford.
- Risk: High
    - It can lead to service disruptions affecting the entire IT environment.
- Likelihood: High
    - This vulnerability is well-known to threat actors.

Company B vulnerability #2

Company B has an Operating System (OS) End of Life (EOL) Detection vulnerability, which threat actors can exploit this vulnerability because it can expose the company to OS vulnerabilities that are not patched or updated. An EOL operating system is one that is no longer supported or maintained by the vendor. This means that the vendor will no longer release security patches or updates for the system, leaving it vulnerable to known and emerging threats"(Mittal, 2024). This could compromise the entire IT environment.

- Impact: High
    - This is categorized as high because it exposes the entire IT environment and could lead to major exposure of data and sensitive information.
- Risk: High
    - This is categorized as high because the attack surface of a threat actor becomes larger since it can affect the entire IT environment.
- Likelihood: High
    - This vulnerability is well-known to threat actors.

Requirement C



Requirement D

Topology Diagram Referencing the layers of the OSI model and TCP/IP protocol stack:

- Firewalls:
    - OSI:
        - Layer 3(Network)/Layer 4(Transport)
    - TCP/IP:
        - Layer 2(Internet)/Layer 3(Transport)
- Router:
    - OSI: Layer 3(Network)
    - TCP/IP: Layer 3(Transport)
- Wireless Access Points:
    - OSI: Layer 2 (Data Link)
    - TCP/IP: Layer 1(Network Interface)
- Switches:
    - OSI: Layer 2(Data Link)
    - TCP/IP: Layer 2(Internet)

- Servers/Web Server:
    - OSI: Layer 7(Application)
    - TCP/IP: Layer 4(Application)
- User Devices:
    - OSI: All Layers(1-7)
    - TCP/IP: All Layers(1-4)

Requirement E

During the merger of Company A and Company B networks, there was some repurposing, adding, and removing of components that could benefit the overall security of the newly merged networks. Some components were removed because of security issues that could be exploited, and other components were added to mitigate those risks. The repurposed components had good security and were at no additional cost, helping to stay within the budgetary constraints.

Repurposed Components for Company A

- Fortinet Next-Gen Firewall: The vendor is reliable with their products and is constantly updating/supporting their devices also would be of no additional cost.
- Laptops and Windows desk: Company A has 75 Windows 10 Pro workstation devices and 20 that are set for remote access, whose OS is still supported, which would be of additional cost. Company A also has 30 Laptops, 6 of which are currently running on an updated OS (Windows 11) and the rest of the 14 are running on Windows 7, which will eventually need to be upgraded but currently at no additional cost.

Repurposed Components for Company B

- Sophos XG Firewall: Company B has two of these devices that are from a reliable vendor and could be used for both companies during the merger for a layered defense of the network. Also would be of no additional cost.
- Stacked Switches: Company B owns three of these devices that could be reused since it's still supported by the vendor and is getting updates. Also would be of no additional cost.
- Workstations: Company B has 75 workstations that are currently running on Windows 10/11 Pro, which are all still supported but Windows XP is an old computer and its hardware may be outdated and will eventually need to be upgraded after the merger. This can be done incrementally after the merger. So currently no additional cost.
- Pooled Printers: Company B is utilizing these devices and are not a threat to the newly merged network since they will only be used internally, also would be of no additional cost.

Removed Components from Merged Network

- Routers: Company A is using a Cisco 7600 which Cisco has announced is EOL and won’t be supported anymore, Company B uses a Verizon Fios Router which is made more for a consumer household rather than an enterprise company and would lack the security features and configuration necessary which could then be used to exploit the merged companies.
- Switch: Company A is using a Cisco 3750X, which has also been announced as EOL and won’t be supported anymore, and if used in the newly merged network, could lead to vulnerabilities that can affect the entire network.

- Wireless Access Points: Company A is using Meraki MR 28 which is know to have vulnerabilities that threat actors utilize to establish an interactive session to devices with elevated privileges.
- Cable plant: Company A is using an outdated cable 5e, which can lead to performance issues.

Added Components from Merged Network

- Sophos XG Firewall: Following the Zero Trust Principle and adding an extra layer of defense before access to the internal network, an additional cost of $949.05
- Cable plant: Removed the cable 5e that Company A was using and upgraded them to the same cable Company B is using, cable 6e, which is going to be an additional cost of $239 per 1000ft, will allow for better performance on the network.
- Wireless Access Points: Added 2 new secured Cisco Catalyst 9120 AX Series, which have no known major vulnerabilities, are well supported, and also have great features for security. An additional cost of $785 for each, totaling $1,570.
- Servers: Both Company A and Company B want to move services to the cloud as part of the new structure of the infrastructure of the newly merged network. Utilizing AWS cloud services will allow scalability and redundancy for both companies. For the migration, an estimated $2,000 to $5,000 is expected. For safety measures, we're going to overestimate just in case of any unforeseen reasons and spend $2,300 for the month, totaling $27,600 for the whole year. This will allow the company to utilize all the best services for security and also be able to scale faster in the future.

Requirement F

In the network proposal, there are two network principles applied that were essential in securing the newly merged networks, Zero Trust Principles and Defense in Depth.

Zero Trust Principle

The Zero Trust Principle was applied based on the requirements of the executives and also the importance it plays in IT environments. The principle of "never trust, always verify" is key to implementation because it addresses the importance of the perimeter-based structure that Company A had, it increases visibility over user activity and devices, and also helps secure remote access devices.

Defense in Depth

The Defense in Depth principle was applied to add layers of security throughout the network adding different security measures through the network such as firewalls, segmentation, and MFA. To avert threat actors from attacking the network and also include redundancy to make sure that import security components are backed up. Defense in Depth also helps reduce the likelihood of one single point of failure in our security network that can mess up operations.

Requirement G

The proposed merged network topology addresses two very important regulatory compliance requirements that the newly merged company must adhere to, such as GDPR(General Data Protection Regulation) and HIPAA(Health Insurance Portability and Accountability Act)

GDPR Regulatory Compliance

The General Data Protection Regulation is a European policy that was created to protect user data in Europe, As Company A is a global company it would likely have European customers where they would have to adhere to this policy. The GDPR is very strict and the newly

merged company network is adhering to the requirements by securing user data with security principles such as Defense in Depth and the Zero Trust Architecture of the network.

HIPAA Regulatory Compliance

The Health Insurance Portability and Accountability Act is a U.S. law that was created to protect the data and information of citizens. With the newly merged network, "AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use the secure AWS environment to process, maintain, and store protected health information"(AWS, 2024). Since AWS cloud services are the cloud service of the newly merged company it allows it to be compliant with HIPAA.

Requirement H

The newly merged network has made many improvements to security but there are still some emerging threats that could potentially affect the IT environment of the merged network.

Advanced Persistent Threats (APTs)

APTs are highly technical and operational attacks that could take months or years and are usually done by groups. APTs will also repeatedly target the same organizations, agencies, or governments and adapt their tools, tactics and strategies over time to defeat defenders. In this sense, it becomes a true cat-and-mouse game" (XM Cyber, 2024). They typically target businesses that have classified data, sensitive data, and PII (Personal Identifiable Information). This is all the information that the newly merged company has; some of the potential network security issues that could be exploited are the End of Life operating system, and some unpatched vulnerabilities (Apache Tomcat Ghostcat Vulnerability). To manage this risk, the newly merged companies must upgrade their EOL operating system, patch the identified vulnerabilities, and document them as soon as possible.

Insider Threats and Access Issues

There's a report that states that "60% of Data Breaches Are Caused By Insider Threats"(Watchdog, 2024). This shows how dangerous and unpredictable insider threats can be, looking at the risk analysis before some network security issues could be exploited, all the users have local administrative privileges in both Company A and Company B that allows for a higher chance of impact and attack for insider threat since they already have access to such privileges, user accounts that are not being used are not removed in Company A which can leave backdoors for insider threats to utilize to exploit the company. To manage this risk, the newly merged companies must implement and enforce the least-privilege principle and also remove unused accounts as soon as they no longer need access to the IT environment.

Requirement I

The newly merged network, based on the scenario and budgetary requirements, was based on the risk analysis and diagrams provided by both Company A and Company B. There were many vulnerabilities that both companies identified and needed addressing, which the newly merged network structure has taken into account. Some important vulnerabilities that were addressed and should be improved upon in the newly merged network for Company A are updating End-of-life devices, creating proper user privileges to not give access to not give administrative accounts to unauthorized users, implementing IAM multi-factor authentication, and closing ports. Importance vulnerabilities addressed for Company B were weak passwords change enforcing IAM multi-factor authentication, also updating End-of-life devices. Now, to analyze and look at the cost-benefit of on-premise and cloud infrastructure solutions, we need to look at the direct and indirect factors that arise from these options. For on-premises, the direct factors are the hardware cost, maintenance, and the physical space required. Indirect factors

would be the scalability challenges and having an in-house team to manage the infrastructure. Now let us look at direct factors of cloud infrastructure, monthly or annual costs for cloud services, charges to move data around, and storage fees. Now the indirect fees, are easy to scale up or down, and no need for an in-house team. If we compare the two there are more advantages with cloud solutions since there's no upfront cost, easy to scale, and more available security features. This also aligns better with budgetary constraints set by the executives of the newly merged company.

The topology proposed implements all the specifications desired by the executives by offering Zero Trust Architecture, cloud capabilities, and overall better network security, Defense in Depth, the least privilege principle, and IAM multi-factor, while also being compliant with all the regulatory compliance needed to properly operate in both the financial and medical sectors.

References

Chow, E. (2022, January 6). The Risks of Open Ports - Eric Chow - Medium. *Medium*. https://eric-chow.medium.com/the-risks-of-open-ports-b1da14a7bd48

Villanueva, M. S. (2024, March 27). *Why Port 3389 is a No-No for Remote Desktop*. https://www.itsasap.com/blog/avoid-port-3389

Sharadin, G. (2023, December 20). *Remote Code Execution (RCE) | Types, Examples & Mitigation | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/remote-code-execution/

How to identify and respond to end-of-life and out-of-service operating systems? - Cyber Defense Magazine. Available at: https://www.cyberdefensemagazine.com/how-to-identify-and-respond-to-end-of-life-and-out-of-service-operating-systems/ (Accessed: 06 September 2024).