OTTOMAN EMPIRE

To: Ima Hacker, Chief Security Officer
From: Luke Laricy
Date: Wednesday, June 4th, 2025
Re: Lost in the clouds? (Question A2)

Ima,

I understand you are interested in knowing about the security trade-offs that we will face if we move our on-site operations to a commercial cloud vendor. That is a valid and responsible question; I would expect nothing less of our chief security officer. I will be happy to share all the info I can with you.

Recommendation

There are certain security trade-offs we will face if we move to cloud. There are certain aspects in which we will be slightly less secure. However, I feel that the uptick in productivity and huge cost saving will more than make up for the tiny amount of security we will lose. Furthermore, I think it may be argued that our data will be even more secure in the cloud. This is why I feel that even with the drawbacks, the decision to move to the cloud is the right one.

Background

The first thing we should consider is what are the pros of keeping all of our servers and data on premise. The biggest one is that we have complete control over our data. We control the machines that data is stored on. We control the security measures regarding those machines. This is not the case if we choose to use an IaaS provider to replace our hardware. The cloud provider will be in control of the machines, and they will provide the security. However, if we choose to use a reputable cloud provider, such as AWS, Azure, or Google, then we can be all but guaranteed that their security will be sufficient.

"Cloud Security at AWS is the highest priority. As organizations embrace the scalability and flexibility of the cloud, AWS is helping them evolve security, identity, and compliance into key business enablers. AWS builds security into the core of our cloud infrastructure and offers foundational services to help organizations meet their unique security requirements in the cloud." (AWS, 2019)

The dedicated lines that we move data back and forth on now is another pro that we have going for us when it comes to security. Our own private leased lines give us the peace of mind that unless someone physically hacks our equipment, we will be the only ones who can see our data. Once again, however, modern day cloud services offer secure solutions such as Azure Key Vault that can ensure that the data we send to and from the cloud is encrypted and unreadable by would be miscreants.

There are also some cons that we have to consider with our on-premises data solutions as well. The first being that our in house severs are a single point of failure. There has been an uptick in the activity of internal threat actors lately. All it would take is a disgruntled employee with an axe and a bucket of water and our site is shut down. A major cloud provider will provide redundancy that will provide piece of mind that our backups could only dream of.

Finally, our email solution is severely outdated. MS-Exchange does not come anywhere close to providing the protection we would get from a SaaS provider such as Microsoft 365.

"To help reduce junk email, EOP includes junk email protection that uses proprietary spam filtering (also known as *content filtering*) technologies to identify and separate junk email from legitimate email." (Microsoft Learn, 2024)

With our current email solution, not only is the email not filtered for spam or junk mail, but we do not have a built-in virus solution like Microsoft Defender. If an employee opens the wrong email, our whole system could be compromised.

Resources

Microsoft Learn. (2024, April 24). *Anti-spam protection - Microsoft Defender for Office 365*. Learn.microsoft.com. https://learn.microsoft.com/en-us/defender-office-365/anti-spam-protection-about

AWS. (2019). *Security and Compliance - Overview of Amazon Web Services*. Amazon.com. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html

Microsoft. (2024, March 27). *Data security and encryption best practices - Microsoft Azure*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

Kumar, Rajeev. "Class 10 BYOD and Other Trends." *IS324*, 3 June 2025, DePaul University, Chicago. PowerPoint presentation.