Cloud Security Architecture Plan

Professor Jeff Baldwin

Michael Lambinicio

4/28/2025

Table of Contents

Executive Summary

Organizations are converting their traditional methods of selling products to consumers. Today, that switch is moving to the cloud computing world. This new method has become increasingly popular over the years as it can seamlessly provide instant services to your business without increased costs such as renting a building, purchasing all the hardware, starting up the initial services and applications and managing security. The infrastructures, Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) are cloud services that are provided and have different features and responsibilities based off the needs of the consumer. These services are provided by providers such as Amazon Web Service (AWS) that has a dedicated platform to ensure high level of quality and security are always first priority.

Introduction

Best Clothes Online Inc. (BCO) is currently a medium-sized company that is considering pivoting their online business into a more robust way of operating without having to incur higher expenses. This transition can be very sensitive as their whole infrastructure will be converted to an alternate way of cloud servicing for the staff and consumer. Also, the scalability of cloud computing makes it an obvious choice with high upside and reduced downside. Understanding which cloud service model to choose from will also help BCO to decide which would be the most beneficial in keeping the high level of security and assurance to respond to all incidents without loss of uptime and increased expense. Big name cloud service providers such as Amazon (AWS) are just one of many that can assist BCO in continued growth of success.

Statement of Need

Due to the possible increase in demand for BCO's services, the organization may need an alternative solution to better scale their services as they may have outgrown their original operational abilities. Managing their own hardware, data centers, facilities, servers, software and security measures will eventually become costly as maintaining your own will require upgrades in physical hardware and possible new facility, to name a few. As the company grows, it would be best to consider a Cloud Service Provider (CSP) to assist in tackling this concern as it can scale your needs on its own high end data centers without incurring high costs.

Assumptions

BCO is already aware of the situation they are in, and they have been given some knowledge on the next measure as their business is expanding. They have already been informed about how advanced and fast technology is moving that cloud computing is the future for markets. They have been educated that using a cloud service provider will be beneficial in their business due to the fact of convenience, scalability, ease of use and cost will continue the success of their business. It has also been recommended to use a major company such as Amazon Web Services (AWS) to assist their needs as they are world-renowned.

Proposed Cloud Security Service Model

From all three models, Infrastructure as a service, Platform as a service, and Software as a service, software as a service would be the best fit for BCO. They can monetize the on-premises location and physical hardware they own and invest it in Amazon Web Services as they have data centers that can provide all the servers and security measures needed to still operate their business. Some of the big benefits that BCO can take advantage of through a cloud service provider is the scalability of the needs. It would be cost effective to get the exact services needed without overspending on the extras that are not needed. All updates and maintenance are handled by the provider so it's less involvement and you can develop a bigger IT team to handle more important issues. Applications are available on-demand through administrators so each workstation or staff member can gain needed tools in an instant. You also do not have to worry about any installation or upfront costs, essentially a win for team BCO.

Proposed Deployment Model

For BCO, the best option would be to migrate their entire data center to a cloud-based operation. During the transition period, roughly about six months, a hybrid solution is viable to ensure everything is crossed over, test pilot all services to ensure a smooth operation and maintain consistency through the cloud. Once the comfort is there and transition is complete, then closing their own servers will be more cost effective and prevents from wasteful manpower to maintain extra resources. Using a cloud service provider such as Amazon Web Services will provide all the necessary services along with all the maintenance for their physical hardware to prevent all their customers from having to deal with it. To add, enabling a public cloud will add additional storage, processing power and applications through Amazon.

Proposed Cloud Security Services

When migrating over to cloud service provider services, they offer a huge benefit when it comes to handling all hardware and networking everything together. In a SaaS model environment, the provider can handle mainly all aspects of networking and physical data centers along with their software, which will allow you to handle all user access and data needed to store on their data centers. The provider will handle all updates and security for applications, guest operating systems, virtualization, network, infrastructure security, security validation, defense-in-depth and disaster recovery plans (Kollaikal & Jimenez, 2024). This takes a huge amount of weight from the consumer, allowing them to focus on who can access their systems and making sure their data isn't getting stolen.

Incident Response Planning

By definition, an incident response plan is a “set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information systems.” (Polymer, 2022) In order to maximize an effective plan, there are some who have developed one that you may deploy below:

1. Define legal frames – Identify the key incident response guidelines required by relevant laws.
2. Perform security risk assessment – pinpoint and address immediate vulnerabilities in your security framework.
3. Establish your incident response team – for their roles and detailed responsibilities at all stages of incident response.
4. Define what a security incident is – what events are considered security incidents, their severity, etc.
5. Implement security monitoring tools and systems - Evidence of incidents can come from log files, error messages, or intrusion detection systems.
6. Establish short-term and long-term containment measures - Short-term measures, like disconnecting affected systems or powering down routers, would limit the damage as soon as possible and limit the incident before it gets worse. The long-term measures, in turn, would allow organizational operations to continue. These include removing accounts and/or backdoors left by attackers on affected systems, installing security patches, and doing other work to limit any further escalation.
7. Establish a clear incident communication procedure - key staff, like management or system administrators, have enough time to gather evidence and prepare for the next steps.
8. Establish documenting procedures - responders can document everything that they are doing and be able to answer Who, What, Where, Why, and How questions.
9. Prepare recovery strategies for situations - may include implementing regular backups of all critical data ensuring that backups are stored securely and separate from the primary network.
10. Refine your incident response plan - After managing an incident, review it thoroughly to enhance your IRP with better strategies, procedures, and scenarios.

(Harrahill, 2025)

Disaster Recovery Planning

A disaster recovery plan is essential for any organization to recover and protect important data within the organization. Redundancy is always offered through your cloud service provider so that should always be a priority added service when setting up. You can also create extra redundancy in case the cloud provider has issues also in which you may also have a separate server located elsewhere and have an image encrypted and saved, but paying for the extra server must be taken into consideration.

Cost Estimate

There are many variables that will dictate how much it will cost a consumer for a cloud provider's services. One would be what services are the most important to have to ensure their data isn't compromised and is kept safe and second will be the cost to use these services. It also must be considered for any fees that may be latched on also such as exit fees, data transfer fees, costs for multi-cloud and hybrid-cloud and the obvious focuses such as how much storage, type of networking and computing. Cloud providers can also provide their own costs as a bundle. So, you may have a choice of On-Demand, where you pay as you go, or reserved, where you may get a discounted rate for committing for a certain period. Most providers also do competitive pricing as they will always try to be the best in the market. So just a little research and comparison of companies will help leverage your needs and price you want to pay.

Resource Planning

BCO would likely have to have a combination of a Managed Service Provider who can train specific internal staff to have them become the "IT team" and have the team maintain the skill and knowledge to train other staff members in the organization. Like a domino effect, this will allow the execution of foundational training new employees must have and develop and increase growth of the business.

Proposed Timeline

Depending on how much service the provider needs to provide, BCO should have a recommended 6 months for a full transition into AWS cloud services. To make it as streamlined as possible, there are key steps to migration.

1. Current architecture assessment
2. Migration model selection
3. Data migration
4. Modernization strategy selection

(Zheldak, 2025)

In these steps, it is advised to take step 1 during the first month. Step 2 would be suggested to use a layered migration model and to organize what applications and services you may need and where to have them using a multi-tenant structure. Then, you can migrate it in stages into a multi-tenant structure overtime, allowing gradual optimization of the system while continuing service to your customers. This process should be about 2 months. Thereafter, step 3 should be spent on migration process through the next month. The last 2 months may be spent on step 4 and any training needs to be given to keep up with the transition. (Zheldak, 2025)

Conclusion

BCO would greatly benefit from the transition into cloud computing and services. It's easily accessible, making mobility and availability effortless for the staff and customers. You can scale what is needed for your organization and eliminate unnecessary ones that would have extra costs. You also have dedicated teams within the cloud service provider to handle all the maintenance and updates on their data centers and software, enabling you to utilize your IT team to focus on more priority items such as higher monitoring and increased security protection of data. You can also be cost effective and use the spare funds in different areas such as promotions of your business, etc. The modern day is now about how fast you can get a service and cloud computing will deliver that.

References

Straub, S. (2024, November 5). *Cloud costs: Price Factors, hidden costs & pricing models*. N2WS. https://n2ws.com/blog/cloud-costs

Zheldak, P. (2025, February 13). *SAAS migration strategy: [why move to SAAS and how to do it]*. SaaS Migration Strategy: [Why Move to SaaS and How to Do It]. https://acropolium.com/blog/saas-business-model-what-is-it-plan-for-migrating-to-saas/

Kollaikal, P., & Jimenez, M. (2024, January 16). *SaaS cloud security: Know your responsibility*. Oracle Blogs. https://blogs.oracle.com/cloud-infrastructure/post/saas-cloud-security-know-your-responsibility

Harrahill, N. (2025, January 17). *How to create a cybersecurity incident response plan*. Spin.AI. https://spin.ai/blog/creating-an-incident-response-plan/