Considerations when Choosing Between Hosting On Premise or in The Cloud: White Paper

Buffalo Computer Graphics, Inc.
4185 Bayview Road
Blasdell, NY 14219
716-822-8668
ebaczynski@bcgeng.com
www.bcgeng.com

Contents

Introduction

Traditionally, organizations implementing large scale technological solutions needed to have the IT infrastructure necessary to host the solution themselves. This meant dedicating time, space, money, and resources to purchase and maintain all the necessary hardware to host the solution as well as providing IT support to employees. The recent wide-scale availability of cloud hosted solutions has dramatically changed the way organizations look at procuring software solutions.

Generally, cloud hosted solutions provide a lower barrier to entry for organizations looking to purchase software solutions. Upfront costs are significantly lower and, if a product does not work out, they can simply end their contract without worries about how much money was sunk into hardware.

Cloud solutions also offer easier management and maintenance of a technological solution as these functions are outsourced to agencies with dedicated staff and resources. However, outsourcing these functions also means giving up sole control of an organization's data and the security of that data. For organizations that already have the necessary infrastructure and well-established IT procedures and policies, the move to cloud based solutions may not seem worth the risk or may even end up costing more money. For organizations that have to follow government mandated procedures, it can be hard to decipher if a cloud hosted solution will meet all the necessary requirements.

The choice can be daunting with the need to consider up-front costs versus long-term costs and to balance the desire for full control versus lowering time commitments from IT staff. The amount of information and misinformation on the Internet about "the cloud" can make the decision even more challenging! In this paper, we hope to help those organizations searching for an answer to cut through the noise, so that they can make a well informed decision about what solution is best for their specific needs and organization.

In this paper, we will explore the questions that Emergency Managers and IT Directors should consider specifically when implementing a Crisis Information Management System (CIMS) and deciding between deploying a cloud hosted or on premise solution. This paper does not intend to list all of the items for consideration, but to raise questions frequently encountered by Buffalo Computer Graphics in various Requests for Proposals and other client inquiries. We encourage agencies seeking a solution to do their own due diligence before making a purchase.

The paper will address three main categories - cost, time, and security. From there, we will explore the implications and considerations of each.

Cost

Cost is often a predominant concern when deciding between on premise and cloud hosting. However, it is important that organizations do not jump to conclusions regarding which option is “cheaper” without considering all factors. Despite the perception that cloud hosting is always less costly, there is no one-size-fits-all approach to answering whether or not it will always cost less than an on premise solution. Rather, the monetary impact of a solution will be determined based on an organization’s unique needs combined with their current infrastructure and existing enterprise licensing agreements. There are four main factors that impact cost to consider when choosing a solution – initial investment versus ongoing cost, hardware costs, software costs, and personnel costs.

Initial Investment vs. Ongoing Cost

The implementation of a cloud hosted solution generally has a much lower initial investment than an on premise solution, especially for organizations that do not have existing infrastructure. This is because organizations hosting a solution on premise must invest in the infrastructure to host the solution. That being said, an important distinction must be made between initial investment and ongoing cost, which ultimately affects the cash flow of the organization.

Most organizations see the cost of cloud hosting simply as a monthly maintenance fee, and the cost of on premise hosting as the cost of hardware and software. However, there are several less obvious considerations. For example, how might the cost of in house maintenance for on premise servers differ from a monthly cloud maintenance fee? How might downtime due to failed servers or a security breach affect productivity and opportunity cost? What do the overhead costs look like? How might an infrastructure investment be depreciated? Some organizations may find, depending on their infrastructure, that an on premise solution has lower ongoing costs than the cloud, and may consider this beneficial. Regardless, the pros and cons of each should be weighed for both on premise and hosted solutions, and should be factored into the equation before making a decision.

The distinction between initial investments and ongoing costs also comes into play for organizations receiving grant funding for their solution. These organizations should consider the funding schedule, and how different levels of initial investments or ongoing costs may affect or be affected by such schedules.

Hardware

Organizations considering an on premise solution should ask themselves, “Does my organization already have suitable hardware in place to leverage, or will I have to purchase new equipment?” When asking this question, they should keep in mind the costs of upgrade aging

equipment, commonly done every three years. Such hardware upgrade and maintenance costs should be factored into the total CIMS cost.

It is typical for a CIMS to need to be able to support a high number of concurrent users in the event of an incident, and this number is typically directly related to the hardware infrastructure required. Even organizations with existing infrastructure may need to purchase upgrades or additional hardware to support the level of concurrent users they will need if that number is greater than what their current infrastructure is capable of supporting. However, organizations that utilize virtualized infrastructure may already have adequate resources to simply scale the solution up during times of high demand. Typically, virtualized environments provide a better cost benefit to organizations when compared to utilizing dedicated hardware for each unique application.

It is easy to overlook some of the hidden costs beyond the hardware itself when making an initial decision. One such hidden cost is electricity – both for powering the servers and for keeping them cool. This typically adds several hundred dollars per year per server to the cost of hardware. Additionally, in the event of damaged or defective equipment, organizations may find themselves with increased downtime, thereby adding to increased opportunity costs on top of repair costs. A virtualized environment may provide some benefit to the organization in its ability to quickly recover from a hardware failure.

The cost of communications equipment (bandwidth), backup power generators, air conditioners, humidifiers, security appliances, storage devices, server racks, and networking equipment also come into play. Hardware can especially become very costly for organizations with a sprawling geographical footprint who might require multiple servers in various data centers (e.g. for failover).

While these hardware costs add up, leasing hardware space from cloud hosting companies can become costly as well. Typically, hosting providers build out very large hosting environments in order to leverage economies of scale and provide competitive pricing to customers. But depending on the contract, monthly costs may increase over time and organizations should carefully consider their contract terms and factor in such potential increases. One common cause of a cost increase is that the initial cost quoted ends up being different than the actual cost for meeting an organization's requirements. Because of this, organizations should be sure that all of their needs are explicitly stated in the contract and priced out to avoid a discrepancy and subsequent fee increases.

Organizations opting for a cloud hosted solution may need to purchase additional computing resources from the cloud hosting company in the event of an incident requiring a high number of concurrent users. This typically comes at an additional cost which can be temporary or long-term depending upon the cloud hosting vendor's business model. While either approach may require downtime for updates, cloud hosting vendors typically provide a guaranteed level of

service aimed at minimizing unscheduled downtime. This is usually communicated to customers in terms of a Service Level Agreement (SLA) which states the guaranteed level of uptime, and higher uptime guarantees typically result in a higher cost of services. Some SLAs also provide for refunds in the event that the service level guarantee is not met. Organizations should compare the SLAs their internal IT department can provide with those that a cloud hosting vendor can. Also, organizations should be reasonable when defining the terms of the SLA, understanding that it will directly impact cost.

Software

There are several software considerations when choosing between cloud hosting or on premise hosting beyond the software itself. For one, database licenses and user Client Access Licenses (CALs) will most likely be required to gain access to the system, each with accompanying costs.

An organization should also consider whether they already have an Enterprise Licensing Agreement with associated vendors that can be leveraged. This will offer the organization greater flexibility in purchasing or leasing software they need. If not, they will need to budget for these third party software applications, keeping in mind that they may also require software maintenance at an additional annual cost. However, organizations should take precautions as to not pay for these licenses twice, as some may be included in cloud hosted solutions as part of the hosting fee. For example, those in search of a CIMS will find that these systems commonly require Microsoft SQL Server and access to Microsoft Exchange, and that the costs are already included in their cloud hosting fee. Along with paying for these applications licenses, those who opt for on premise solutions may find that they will need to purchase the operating system license for their servers as well. Again, most cloud hosting vendors include these third party licensing fees in their monthly service fee.

As a CIMS typically requires the use of Geographic Information Systems (GIS), organizations should compare and contrast costs that result from leveraging their own GIS software and related infrastructure, or from utilizing ESRI's ArcGIS Online. Generally speaking, GIS software can be costly to maintain and requires special personnel to install, maintain, and operate. Organizations that do not already have an enterprise GIS solution and staff, may find it beneficial to look into leveraging ArcGIS Online.

Finally, organizations must consider the cost of the CIMS itself. Will they be purchasing or leasing the software? Purchase, maintenance, and Software as a Service (SaaS) prices will vary and influence the overall spending forecast accordingly. For example, some software vendors may include maintenance and upgrade costs in their monthly SaaS fees, while organizations who purchase software licenses may have to pay a separate fee to update their system. Additionally, some software vendors may have policies where cloud customers cannot purchase certain features without moving to a higher tier level of the system. Organizations will therefore want to carefully consider what is included with each procurement option.

Personnel

Skilled personnel, whether they are on staff or third party consultants, are costly necessities for both cloud hosted and on premise solutions. When deploying on premise solutions, highly trained and generally expensive employees or consultants are required to install and maintain hardware and software. These are necessary services, and organizations should consider how their department will be charged for them. Additionally, for organizations who host their solution on premise, time will be required on an ongoing basis to maintain server operating systems, anti-virus software, and general upkeep of the servers. Either staff salaries or third party contracting costs will be affected accordingly. Organizations who host their solution in the cloud are not immune to these costs – they will need to pay the cloud hosting company for configuration and support in lieu of using internal IT staff, though these costs may be lower overall.

Time

Beyond cost, organizations will discover that hosting on premise or in the cloud will have different results regarding time commitments – both during implementation and during use.

Time to Implement

Organizations should take into account the immediacy of their CIMS need when deciding between on premise or cloud hosting, as the length of time it takes to implement the system varies greatly between the two. While an organization choosing an on premise solution may have the infrastructure in place to host a solution, it is easy to overlook the actual logistics of installation – including the multiple teams that will need to be coordinated and the time it will take for new hardware to arrive. It is important to ensure that on premise servers have ample space and proper permissions set up ahead of time. Additionally, the vendor will need to access the server for installation, configuration, and maintenance, and therefore the organization should already have a VPN established by installation time. Depending on how the remote access is controlled, it could add additional limitations to the vendor's ability to support the application. Other delays can often result from reasons such as hardware procurement, architectural design, hardware provisioning, security reviews, and project management time. While not an absolute, cloud hosted solutions can typically be implemented very quickly when compared to on premise solutions.

Scalability

A CIMS needs to be able to scale up in an emergency and handle the maximum amount of concurrent users needed. In these urgent instances, there is no spare time to procure and install additional equipment or software. In the event that an organization is using virtualized hardware for their on premise solutions, scaling up is able to be done relatively quickly. However, if dedicated hardware is being utilized for an on premise solution, that hardware may

need to be upgraded or augmented, which can take considerable time unless properly planned for in advance.

Cloud hosted environments are typically designed to scale quickly should the need arise. This, however, is often at an additional cost and should be discussed with the CIMS vendor and the cloud hosting provider in advance when making a decision. Finally, organizations should discuss with the CIMS vendor about exactly what is required to scale the solution to support additional users. Each application scales differently, and prior knowledge of what is required for scaling up will be critical should an on premise solution need to do so during a crisis.

Support

System support, maintenance, and updates will differ in both time and cost for on premise and cloud hosted solutions. Organizations who opt for on premise systems typically use up many of their internal IT resources for performing support in the event of an issue and overall system maintenance. While these resources are costly, this means that these organizations are able to fix issues more quickly and on their own schedule rather than waiting on vendor support.

System updates, however, will generally happen more quickly for organizations hosting on the cloud. These updates are usually delivered as soon as they are available, whereas updates for on premise systems are scheduled to be delivered at the convenience of the organization's IT staff.

Having support available when needed is critical, and organizations should discuss support response timeframes, including business hour and after hours support requirements, with both internal IT staff and the CIMS vendor. Each will be able to provide their support methods and response time commitments.

Security

Data security, of course, plays an extremely important role when it comes to deciding between cloud hosting and on premise hosting. Here, we will look at the possibility of security breaches, what should be discussed with data centers, how the level of data control differs for on premise and cloud hosted solutions, and what to consider about an organization's current IT environment.

Security Breaches

While data security is extremely important to any organization, agencies dealing with especially sensitive data may need to take extra precautions to ensure proper handling. These considerations are not unique to just those hosting their data with a third party hosting company - organizations hosting data within their own servers should also have a proper communications hierarchy in place to minimize security issues and resulting complications. Organizations should understand how and when they will be notified when an intrusion is

detected, whether on the cloud or in their own server. They should also know how and when data is encrypted, whether in motion or at rest. By doing so, organizations can be better prepared in the event of a breach.

Data Centers

Deploying a cloud hosted solution means relying on the security of a third party data center. It is therefore imperative to know all certifications held by that third party, and to review these certifications with a legal team to confirm what preventative measures are being taken by the hosting company, and who is responsible for what in case of a security breach.

The physical location of the data center should be considered for two reasons – first, for the physical security of the data and second, for administrative and legal purposes. In terms of physical security, organizations may want to consider whether or not the data center is located in an area with a risk of natural disaster, such as a hurricane or an earthquake. If so, does the data center have proper backups in place? The organization should also have a full understanding of how and when data recovery will be provided in the event of a disaster.

Organizations that opt to host their data with a company that uses data centers in other jurisdictions or countries outside of their own should do their due diligence to understand the legal implications of storing data across borders. These organizations will be subject to the laws of the other jurisdictions and must act accordingly.

As software vendors that offer cloud hosted solutions have typically purchased server space with a preferred cloud hosting company, it is common to share server space with other organizations deploying the same solution. While data remains separate, this may pose a security risk to organizations dealing with especially sensitive data.

Level of Control

Not only does deploying a cloud hosted solution mean relying on a third party's security standards, but it also means relinquishing much control over the organization's data. Those that host their solution on premise benefit by having direct control over their data and its security. This means that they are able to access their data when they want, and are able to put the security precautions into place that they deem necessary. Organizations with an on premise solution are also able to access their system in the event of an Internet outage, unlike those hosting in the cloud. In BCG's experience, this is one of the core reasons those seeking a CIMS choose to host on premise.

Organizations hosting their solution in the cloud may not be able to access their data as freely or as quickly as organizations with an on premise solution. Because of this, organizations may want to pay special attention to the physical location of their hosting provider's data center as time zone differences may affect business hour support windows. These hours and the services provided should be clearly laid out in the Service Level Agreement (SLA), with specific penalties

outlined if the defined services are not adequately met. The purchaser should also be aware of external factors that may impact service but are out of the cloud hosting provider's control that may not be outlined in the SLA.

In addition to access to data while actively hosting, organizations should also have a full understanding of what will happen to their data when they stop hosting. It is advised that organizations discuss with the CIMS vendor and cloud hosting company if and how data will be stored, transferred, or destroyed.

Conclusion

In this paper, we explored the cost, time, and security implications and considerations when choosing between deploying an on premise or cloud hosted Crisis Management Information System. As every organization is different, there is no one-size-fits-all approach to deploying a CIMS. Each of the three categories of consideration have potential pros and cons that will differ from organization to organization, and we therefore recommend that CIMS seekers explore each consideration carefully before making a final decision as to whether or not they deploy on premise or in the cloud. To help ease this process, we have included a quick reference chart on the following page.

Quick Reference Chart

Factor	On Premise	Cloud
Pricing	Higher initial investment Lower ongoing costs Additional hardware purchases may be needed to support scalability Owned hardware can be virtualized and shared for other internal needs More demand on IT staff 3rd party software licensing costs may be required	Lower initial investment Higher ongoing costs Hardware for scalability is typically already in place at the data center for rapid scalability Hardware cannot be leveraged for other projects Less IT involvement/time spent Typically hosting costs include 3rd party licensing costs
Security & Database Control	Direct control over the database and application data Direct control and responsibility for all application security – may involve higher time commitment Limited or restricted vendor access to the database may slow problem resolution and troubleshooting	Database and application data securely hosted on a remote server Security becomes the responsibility of the hosting provider Direct vendor database access supports rapid problem resolution and troubleshooting
Deployment & Scalability	IT staff control deployment timeline and rollout which often takes considerable time Scalability may take time (planning, hardware procurement, implementation)	Vendors typically can deploy a cloud solution relatively fast Typically hosted sites can be rapidly scaled up using in place computing resources
Updates	Updates are scheduled to be delivered at the convenience of the organization's IT staff	Updates are delivered as soon as available
Reliability / Availability	System internally available during Internet outages	System may not be accessible during Internet outages