CIMPHONI WHITE PAPER SERIES

Cloud Security – Extending Your Cyber Fortress to the Cloud

Dr. Max Boedder

cimphoni

Is your organization considering a move from on-premise systems to the cloud, but concerned about information security? Are you already using the cloud, but uncertain about how well your networks and data are protected? The transition to cloud computing is transforming businesses and IT departments world-wide, yet all too often, security is an afterthought. It shouldn't be.

There have been many examples of data breaches due to security gaps in cloud computing, and one of the most recent was a leading telecommunications company's exposure of more than 14 million customer records. The vulnerability that was exposed to hackers in this case centered on a contact center system that generated log files with confidential data, which was stored at an unsecure cloud location.

Cloud computing seems omnipresent with promises of inexpensive, pay-as-you-go computing and storage resources that are available on demand and are tailored to your needs. There are a variety of cloud computing models available where shared third-party data centers host part or all of your computing and storage infrastructure. Organizations may have their enterprise applications and data distributed across multiple cloud vendors and cloud computing models with limited tools to manage confidential data. In some cases, the information technology function may not even be aware of all of the cloud computing services that their enterprise is utilizing. The lack of oversight of this distributed computing and storage environment is the core cyber security challenge with cloud computing.

"Many organizations lack the information and tools to manage a distributed cloud computing and storage environment. This exposes the company to the risk of a cyber security incident."

Cloud Computing and Heisenberg's Uncertainty Principle

The dynamic and evolving nature of cloud computing adds another dimension when compared to the security of on-premise systems. In physics, Heisenberg's uncertainty principle states that we cannot measure the position and the momentum of a particle with absolute precision, and the more we know about one of these attributes, the less we know about the other attribute. For cyber security professionals, this is what cloud computing looks like:

1. Audit Reports
2. Identity & Access Management
3. Encryption & Key Management
4. Single Tenant or Multi-Tenant?
5. Additional Layers of Security
6. Container-Based Virtualization
7. Migrating Data to the Cloud
8. Integrating with the Cloud

Audit Reports

The first thing an organization loses when transitioning to the cloud is physical access. Because cloud providers typically have many clients, it is not feasible to allow client access to these data centers. Instead, cloud providers often engage trusted third parties, in many cases certified public accountants (CPAs), to conduct a standardized audit and to produce a report in a standardized format. The cloud provider then makes the report available to its clients. The American Institute of CPAs (AICPA) has provided the suite of System and Organization Controls (SOC) framework

(formerly SAS 70) to standardize how CPAs audit and test security controls for effectiveness. A commonly used report type is called "SOC 2® – SOC for Service Organizations: Trust Services Criteria." Recently, the AICPA published a cyber security risk management framework through which CPAs can produce standardized reports on an organization's cyber security risk management program.

When you select a cloud vendor, we recommend that you ask for a recent SOC 2 report and review it to ensure that the cloud services and infrastructure you are planning to use fit your needs and are fully addressed by the report. For instance, the cloud provider's SOC 2 report may only cover its North American data centers, but you intend to use a North American data center as a primary location and a European data center as a backup. The description and effectiveness of the security controls of the European data center would not be included in the SOC 2 report, so you may want to ask additional questions about the European data center. Also, in countries outside of the United States, your data will be subject to local and regional requirements that may, in fact, be stricter, such as European privacy laws.

Identity & Access Management

It can be challenging enough to manage users' identities and access with on-premise systems that range from integrating with Active Directory to having their own application-level identity and access management (IAM), to integrating with single-sign-on (SSO) tools, but with different protocols (LDAP-LDAPS, SAML , etc.). Even some legacy applications from acquired or merged organizations may pose IAM compatibility challenges. For cloud-based systems, these challenges are amplified and more difficult to manage when authentication travels across the Internet, which is unprotected infrastructure. Some organizations leverage cloud access security brokers (CASB), which reside between an organization's on-premise infrastructure and cloud providers' infrastructure. CASBs can be helpful in enabling the migration to the cloud in a distributed IT environment where different departments procure their own cloud-based solutions.

In addition to managing your users in cloud-based systems and protecting authentication information, we recommend that you ensure cloud-based vendors keep audit trails that are consistent with your requirements. Depending on your organization's situation, certain legal, regulatory, or contractual requirements for audit trails may apply, such as Sarbanes-Oxley, HIPAA or PCI. These requirements may include document retention, specific levels of detail and protective measures to ensure the logs cannot be altered. If the cloud vendor's log retention capabilities do not suffice for your needs, you may want to consider importing the logs into your own log aggregation tool. In summary, when selecting a cloud-based vendor, we recommend you ensure that you fully understand how their IAM platform works, how it could be integrated with your organization's own IAM or SSO, what audit logs are available and for how long, and if you can import audit logs into your own tool.

Encryption & Key Management

An important tool to keep sensitive data confidential is the ability to make it unintelligible by using encryption. Successful encryption requires two inputs: a strong encryption algorithm and a strong, secret key. The challenge with using strong encryption algorithms is that over time they become weak and less effectve. Sometimes this happens as decryption software becomes more capable or because someone uncovered a vulnerability in the encryption algorithm. Even if this does not happen, computers are becoming faster and can process increasingly larger amounts of data. Both developments enable hackers to break an encryption algorithm. If your

cloud vendor is still using the encryption algorithm that it used 10 years ago, chances are that it no longer offers effective protection of your data. Be sure to verify they are staying current.

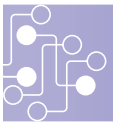
The second component is your secret or private key: effective key management is necessary for keeping keys secure and for periodically changing them. If you are letting your cloud vendor manage your keys, what assurances does your vendor give you that the keys are protected from unauthorized access and use? Cloud vendors offer different solutions, including bring-your-own-key (BYOK), key vaults and integrations with third parties to host and manage your encryption keys. A certain level of responsiblity comes with securing your own key – i.e., if you lose your key, you lose the data. Also, managing your own key may require expensive computing and network resources that may, in some way, negate the purpose of moving to the cloud. On the other side, if you leave the cloud vendor and want to make sure that no one will ever have access to your data, all you must do to securely erase your data is to destroy the key, a process called crypto-shredding. Once the key is destroyed, nobody will be able to read your encrypted data even if it was not completely erased. In summary, before you move any sensitive data to a cloud vendor, we recommend you assess the vendor's encryption methods and key management processes to ensure they will suffice.

Single Tenant or Multi-Tenant?

In a single-tenant architecture, your cloud provider is hosting your instance of the application on dedicated physical or virtualized hardware. Separation of data is maintained at the physical or operating system level. In a multi-tenant architecture, you are sharing infrastructure with other clients that are also hosted by your cloud vendor. Any separation of data is logical and you may have limited options for implementing security controls. Single-tenant architectures may cost more than multi-tenant options, but also may give you more security options. In addition, a single-tenant option may give you better performance, which may be a concern for the timely availability of your system and data.

A virtual private cloud (VPC) typically assigns a separate private IP subnet and thereby provides a degree of isolation, at the network level, between your cloud-based system and any other systems hosted by the same cloud vendor, as well as anywhere else. With a VPC, you can implement security controls based on IP address ranges. In addition, you can easily implement a virtual private network (VPN) between your users and the virtual private cloud.

In summary, there are several options on how to set up a public cloud system. They all have advantages and disadvantages, depending on your organization's situation and needs. You want to make sure that you are making an informed decision about the associated risks and trade-offs.



Additional Layers of Security

An important concept in cyber security is to develop what is called "defense-in-depth." A medieval castle implemented defense-in-depth using an outside wall with a moat and a drawbridge to the gate, an inner wall guarded by better-trained soldiers, and then another wall around the king's court, guarded by elite soldiers. For on-premise systems and networks, such a defense-in-depth is often implemented from the outside in. As an example, an organization may set up a perimeter firewall protecting its networks to the outside, followed by a demilitarized zone (DMZ), then an inner firewall, followed by an intrusion detection system (IDS) or intrusion prevention system (IPS), and then a web application firewall (WAF).

When moving to the cloud, your vendor may only give you limited, if any, options to set up a defense-in-depth.

However, a defense-in-depth approach can still be applied to reduce your risks. Instead of building your layers from the outside-in, you have the option of building up your layers from the inside out. In other words, any connection to your cloud-based system must first pass through a security control before it can reach your cloud-based system. Such security controls can be hosted by your cloud vendor or somewhere else in the cloud. For example, there are a number of hosted web security and email spam/phishing filters available. If you use a cloud-based email system, you can add a layer of security by routing emails through such a hosted email and spam/phishing filter. Your cloud vendor may have relationships with vendors of such add-on systems, which may make it easier for you to manage the integration between them. In summary, depending on what type of system you are moving to the cloud, we encourage you to find out what add-on layers of security are available and to assess if they would help lower your risk of moving to the cloud.

"When moving to the cloud, your vendor may only give you limited, if any, options to set up a defense-in-depth. However, a defense-in-depth approach can still be applied to reduce your risks. Instead of building your layers from the outside-in, you have the option of building up your layers from the inside out."

Moving Applications to the Cloud Container-Based Virtulazation

If your cloud vendor is hosting not only servers and operating systems (know as IaaS and PaaS), but also the actual application, this is referred to as software-as-a-service (SaaS). SaaS has become very popular for delivering, supporting and licensing software. Typically, administrators and users access the application through a web browser.

In other cloud computing models, you may decide to deploy your own applications across infrastructure and/or platforms in the cloud. An increasingly popular deployment model is containerization or container-based virtualization. In essence, you are running multiple isolated systems or containers with an application on the same host and system kernel. Each container virtualizes a single application and creates an isolation boundary at the application level. These containers include all required system components such as libraries, which solves compatibility and versioning problems. Deployment of containers can be very fast, efficient and secure. Cloud containers are becoming increasingly popular for the deployment of applications to cloud-based environments. Different container technologies have different approaches to container security. In summary, if you decide to use containerization, we encourage you to familiarize yourself with the specific advantages and security concerns of the technology you select.

Migrating Data to the Cloud

Regardless of what type of cloud-based system you select and how securely you built out your new cloud-based system, chances are you still need to migrate your data to its new home. In addition, the data may need to undergo some transformation to fit the underlying data model of the new application. You want to make sure that your data does not become compromised or corrupted during this migration process. Data migration to the cloud typically includes some type of encryption to make the data unintelligible to anyone who intercepts it as it is in transit across a public network.

When you use an online data transfer, you need to be mindful that you are probably going to transmit a large amount of data. Both your current data center and the receiving data center in the cloud must have sufficient network bandwidth to transmit and receive the data during the time window you select. In other cases, it may make sense to take a snapshot of your data and start the migration process while continuing to operate the original system. Once the data has been migrated, in a second step, you can migrate the changes that took place since the snapshot was taken. These changes usually involve a much smaller amount of data. If necessary, you may need to repeat this step one more time. The goal is to minimize the time your system is not available while ensuring the integrity of your data during the migration process. These steps need to be carefully planned and coordinated with your cloud vendor.

Another option is to use a physical carrier to migrate data. In this model, the data is exported to encrypted storage media. The media is then placed in a protected case and sent via courier to the cloud vendor. The vendor will decrypt and import the data from the physical carrier and perform any necessary data transformation. In some cases, a hybrid approach may make sense: use a physical carrier to migrate the data at the time of a snapshot (see above) and then use an online migration to transmit changes that took place since the time of the snapshot.

In summary, depending on the amount of data you will need to migrate, you may opt for an online transfer or for transmission via a physical device that you transport via a courier. Whatever your approach, you want to make sure you conduct one or two test runs first to test the transfer mechanism, the encryption method, the data transformation, and the time requirement for the full migration.

"For file-based transmissions, it is not unusual to encrypt the file at rest and then use and encrypted transmission method for the data in motion, using different encryption keys and possibly different encryption methods."

Integrating with the Cloud

Unless all of your data is stored at the same cloud vendor, you probably will need to exchange data with multiple vendors. Depending on your infrastructure, you may need to integrate on-premise systems with cloud-based systems, cloud-based systems with other cloud-based systems, or both. Some companies even use cloud-based integration platforms ("Integration Platform as a Service" or "IPaaS") to integrate with the cloud. Integration options include batch processing via periodic transmissions of files and real-time processing (e.g., via web service calls).

Similar to how you protect the data that you are migrating to the cloud, you also want to protect your ongoing system integrations with the cloud-based systems. For each integration point, we recommend that you determine the sensitivity and criticality of the exchanged data and then determine the appropriate security controls. In many cases, these controls include protected authentication mechanisms and the use of strong encryption methods.

For file-based transmissions, it is not unusual to encrypt the file at rest and then use an encrypted transmission method for the data in motion, using different encryption keys and possibly different encryption methods. It is also a standard industry practice to transmit protected files in two steps: from the protected zone of the network to the so-called DMZ (near the perimeter firewall) and then from the DMZ to its destination. The recipient of the file may have the destination located in their DMZ. In a second step, the recipient would then transfer the file from their DMZ into the protected zone of their network. Regardless of how you integrate with the cloud, we recommend you understand what type of data traverses each integration point and protect each integration point accordingly.

Protect Your Organization's Cloud

As a basic framework for successful cyber security programs, Cimphoni recommends focusing on the areas of the "human firewall" (employee awareness training and proper training on tools), keeping systems updated, building out defense-in-depth, practicing the identification and focused protection of sensitive data, and preparing and practicing an incident management and response plan to be rehearsed and ready for a cyber security event. These cyber security recommendations apply to the cloud as well. Be sure that you include your cloud-based systems as you implement and improve your cyber security program. For example, if you move sensitive data to the cloud, be sure to build appropriate layers of protection around it. Make sure it is clear who is responsible for updating your cloud-based systems – is that you or your vendor? Provide proper training to your employees. And, ensure that your incident management and response plan includes and covers your cloud-based systems.

Along with all the promises of cloud computing comes the reality of significantly increased cyber security challenges. If you are concerned about the confidentiality, integrity, and availability of your systems and data in the cloud, we encourage you to consider the steps described above. Cloud computing can be the right choice for your organization, provided you consider the risk and costs of extending your cyber fortress to the cloud.

"As a basic framework for successful cyber security programs, Cimphoni recommends focusing on the areas of the human firewall, keeping systems updated, building out defense-in-depth, practicing the identification and focused protection of sensitive data, and preparing and practicing an incident management and response plan."

ABOUT THE AUTHOR

Dr. Max Boedder, Partner

Max leads Cimphoni's cybersecurity and risk management practice, helping organizations develop and maintain a strong cyber defense fortress, as well as highly effective cyber incident response plans. Prior to joining Cimphoni, Max was the Director of Enterprise Applications for AAA of Northern California, Nevada & Utah. He has also held several C-level and senior leadership roles in the business process outsourcing (BPO) industry. Clients he has served include Johnson Outdoors, The Kroger Co, Winn-Dixie, Meijer, Aetna US Healthcare, Chase, Capital One, Citibank, Freeport McMoRan Copper & Gold, FedEx Express, FedEx International, Teleflora, Globe Life, SIEMENS, NOAA, Tanger Outlet Stores, the University of Miami, the State of Connecticut and Parago.

Max holds a Master's degree in Computer Science, an MBA from Webster University and a Doctor in Business Administration from the University of Phoenix. He is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified CSF Practitioner (CCSFP). Max is an eight-year veteran and former officer of the German Air Force. He has taught information security at Webster University for over 10 years, serves on the Master of Science in Cybersecurity advisory committee, and is adjunct faculty at the Irvine, CA campus. He likes spending his spare time in the gym where he studies several martial arts. He is fluent in English, German, French and Spanish.

About Cimphoni

Cimphoni is built on the premise that technology, when properly applied and led, can deliver practical solutions that transform businesses and improve the products and services we use every day. The Cimphoni team is comprised of highly experienced technology and business leaders with a thirst for innovation, an understanding of the value and application of new technology, a passion for solving problems and a hands-on approach to execution. Founded in 2012, we serve customers throughout the United States from our offices in suburban Milwaukee.

Contact Cimphoni

If you would like to enhance your cyber security program, please contact us at (888) 470-0448 or info@cimphoni.com. We can help you mitigate risks and build a cyber fortress around your organization and its most critical data.

P.O. Box 80
Hartland, WI 53029

t: (888) 470-0448
e: info@cimphoni.com

www.cimphoni.com

cimphoni