Cloud Adoption:

Security and Risk Considerations for Executive Management

BUSINESS DRIVERS FOR PUBLIC CLOUD ADOPTION

Public cloud adoption has soared in recent years for two primary reasons: agility and scalability. The agility afforded by the cloud is truly unparalleled. Whereas it once took a matter of days or even weeks to provision servers in corporate data centers, organizations can now instantiate those same servers in a matter of seconds in the cloud with unlimited scale. Furthermore, when more resources or services are needed, they are always on tap in the cloud. The systems can be built with today's needs in mind, knowing that they can be scaled up as needed to meet the organization's growth and performance needs. In the old paradigm, IT managers often had to purchase equipment that far outstripped the immediate need in order to meet uncertain future demands. The new ability to rapidly provision and de-provision resources and add capacity where needed leads to efficiency and in many cases, cost savings because you are only paying for what you need

The business benefits of such agility and scalability are many fold. Organizations can rapidly test and prototype new systems. Complex application environments that used to take an eternity to deploy can now take weeks or months to build in the public cloud, where the entire build process can be automated and orchestrated. This allows IT teams to rapidly build and rebuild for testing and development purposes. That speed and agility translates directly to the revenue generating core of any business, providing technology-enabled innovation and efficiencies like never before. However, without proper risk management and a design for compliance, those benefits can easily become risks to the business. Hence, risk management is key to capitalizing on the business-enabling benefits of the cloud.

CLOUD ADOPTION AND BUSINESS RISK

As with any business enabling technology, public cloud adoption poses risks. Senior leaders should understand and manage those risks in a way that is in line with the organization's risk appetite while taking into account the regulatory and competitive factors applicable to the organization and its industry. The following are key areas of risk to be considered.

Security Risk

First and foremost, it is important to understand who is responsible for the security of your data in the public cloud. This general maxim holds true across all public cloud providers: The provider is responsible for security of the cloud infrastructure while you, the customer, are responsible for security of your applications and data in the cloud.

This means the public cloud provider is offering infrastructure and platforms on which your IT team can build systems and applications. You can think of the infrastructure or platform as a set of services available from the provider. The provider ensures the infrastructure those services operate on are available, protected from a physical perspective, and that the services are patched regularly.

Then your IT team will deploy applications and data on those services and allow access to those applications and data, often over the public internet. It is up to you to make sure that security measures for protecting your applications and data are as stringent or more so than those you may use to protect your physical data center. Despite the fact that these are sitting in a public cloud provider's data center, your IT team needs to deploy the same types of security controls and policy that were needed in the private data center in order to adequately protect the environment. The good news is that those security capabilities can be rapidly deployed in the public cloud as well.

Unfortunately, this reality is not always well understood. IT teams, DevOps and application owners, in their desire to reap the rewards of agility and scalability in the public cloud, will sometimes move sensitive business data to the public cloud without first ensuring that the requisite security capabilities that exist in the physical data center can be extended to the public cloud for consistency.

As a senior executive leader, you should ask your IT teams and application owners whether they have extended the company's security policies from the network into the public cloud. Some examples include: virtualized next-generation firewalls, advanced malware prevention, identity and access

management and encryption – the same tools you are using in your on-premise corporate data centers.

Governing access to data is another key security consideration. Your IT team determines who can access your data in the cloud and how. They also determine if the cloud provider itself can access your data.

There is a broad spectrum of control. Access control mechanisms and encryption methods can be used to govern how applications and data can be accessed in many scenarios. For example, applications and data are:

- **Accessible to the general public over the internet.**
- **Accessible on the internet, but only to certain authorized parties.**
- **Accessible only to those internal to both your organization and the cloud provider.**
- *Note: If data is encrypted, the cloud provider has the keys to decrypt it.*
- **Accessible only to those internal to your organization.**

Note: The cloud provider cannot access your data because it is encrypted and does not possess the keys to decrypt your data.

Organizations need to make decisions regarding access control based on the sensitivity of the applications and data placed in the cloud. Implementing proper access control guidelines at the outset will minimize the chances for potentially risky exposure of applications and data.

Compliance Risk

Cloud adoption may also pose regulatory risks for organizations in some jurisdictions. For example, the European Union (EU) has laws governing the movement of personally identifiable information (PII) outside of the EU. Therefore, in some cases it can be a violation of EU law for an organization in the EU to store such data on cloud servers based outside of the EU. Many other countries have similar rules, as well as processes and procedures that can be followed to allow movement of data more freely.

IT teams do not always understand these implications. In one example from a large global company, the US based IT team was in the process of developing a new customer relationship management (CRM) system for the organization. For decades, the system consisted of disparate applications sitting in their private regional data centers around the globe. The IT team saw this as an opportunity to leverage the cloud to converge these systems and eliminate the cost and overhead of maintaining so many duplicates. In no time at all, they were able to develop a rapid prototype of a newly integrated CRM system in the cloud. They did this by simply moving the data from the CRM systems in the U.S. and EU and from the APAC data centers into the cloud, and then merging the data. It was up and running in no time. Unfortunately, the lawyers were also up and running. What seemed like a simple move toward efficiency by the IT team was actually a major breach of EU data protection directives in the eyes of the corporate legal team. Some countries even mandate that such violations be reported to the national data protection authority, which can result in fines.
These risks are all manageable with the right processes in place. IT teams need to keep track of where data resides and they need to seek guidance from a regulatory compliance perspective before moving sensitive data or putting that data to a new use. A strong link is required between IT teams and knowledgeable regulatory compliance experts to provide oversight and guidance for IT projects.

Business Risk

Cloud adoption, if not properly managed and secured, can also lead to operational risks for the business. It is important to consider and plan for all the potential impacts. These will vary by industry, but some of the key areas include:

- Data ownership
- Availability of business critical functions
- Liability for security breaches
- Competitive considerations

Just as you would maintain ownership of physical property that you store with a third party, you should maintain ownership of your business data and applications in the public cloud. Data may be moved to a public cloud-based service by our IT team, but data may also be created in the public cloud. Your agreements should cover both scenarios. It's also important to consider how your data can be extracted from the public cloud service in the event the relationship is terminated. For some systems this is very simple and straightforward, but for others it could require some up front planning and agreements.

Agreements with public cloud providers serving business critical functions should also include service level agreements (SLAs). If your cloud service provider is down, your ability to service customers and generate revenue is impaired. Most cloud providers can share historical uptime performance metrics. Organizations should evaluate those metrics against the needs of their businesses to make sure outages that can be reasonably estimated based on those metrics will not be detrimental to the business. Service level ageements and remedies for breaches of those SLAs can be included in your contracts with public cloud providers.

Legal agreements with public cloud providers will also specify who is liable for various types of security breaches and any limits to that liability. This is an area in which to pay careful attention. Refer back to the section on security risk regarding responsibility for security in the cloud. The shared responsibility

model means that liability for breaches should also be shared appropriately depending on the source of the security breach. But again, the best course of action is to not outsource your security architecture to the public cloud providers but to own that strategy yourself and extend your existing, proven security policies to the public cloud engagement.

Here are the top questions that should be answered in cyber risk discussions with executive management and the board:

1. What is the overall strategy for leveraging cloud resources vs. the corporate data center? (For example: "Cloud first" for anything new? Are you migrating existing applications from the data center to the cloud?)
2. What information/business assets/business functions are being moved to the cloud?
3. Are they critical to business operations? If so, is the viability of your business now dependent on the cloud provider? Is that an acceptable risk? What are your SLAs and recourse for broken SLAs?
4. What have you done to assess the security and reliability of your cloud providers and their downstream providers?
5. Are security controls being implemented in the cloud, just as they would in the data center?
6. Is your existing security policy being extended to public cloud deployments?

MANAGING THE RISK

Communicating to the Board

According to a survey of audit committee members conducted by the New York Stock Exchange (NYSE), only 21 percent of directors agree their company has cybersecurity risk well under control. About 66 percent said their senior IT executive reports to the board only "occasionally." Senior executives and corporate board members should all be apprised of these risks and how they are being mitigated or accepted. In many organizations, IT teams and application owners are making the decision to move critical business functions to public cloud based services without adequate communication to management and the board. This is often the case because the communication of cyber risk between technical teams and non-technical leadership is minimal or non-existent. Organizations need to develop these communication pathways by establishing what needs to be reported to management and the board and by ensuring they have the right staff or advisors to translate technical risk into business terms.

Key Questions for Technology/Security Leaders

Non-technical leaders should know the questions to ask IT teams and application owners about cloud security and risk. It is important to ask these questions because there are times when well-intentioned IT teams and application owners leverage the speed and agility of the cloud at the expense of security. In many organizations, there are well-understood procedures for provisioning new systems into the corporate data center, and those procedures include reviews and oversight from the information security team. Provisioning new systems within a public cloud service, on the other hand, can be done easily and immediately by anyone who needs it. The security or compliance teams may never know that it happened. This is the scenario that leads many organizations down the wrong path. The goal should be to securely enable public cloud adoption by deploying the right set of security procedures and technologies in the cloud environment to preserve your security policies.

Key questions to ask your IT leaders:

1. What types of systems or data are we putting in the cloud? Are they production systems? Test environments?
2. What have we done to ensure the security and reliability of our public cloud service providers? (Note: This can range from an onsite inspection/audit of the cloud provider to simply obtaining third party audit certification reports.)
3. What kind of data are we putting in the public cloud? Customer data? Highly sensitive information?
4. How are we managing access to data and applications in the cloud?
5. Is the data encrypted? If so, does the cloud provider have the keys to decrypt the data?
6. Do we have the same security controls and policy in the cloud that we have in our data center? (For example: virtualized application layer firewalls, intrusion prevention, advanced malware detection.)
7. In the contract or EULA, who is liable for data breaches?
8. Can we control what data our users put into sanctioned SaaS applications and how that information is shared?
9. Are our public cloud providers relying on third parties to provide us service or customizations?

CONCLUSION

The move to the public cloud can enable and transform your business. On balance, the benefits generally outweigh the risks as long as security and risks are properly managed. Security in the public cloud is the responsibility of your IT, application owners, and security team, just as it is in the private data center – and all the same concepts and requirements apply. IT teams and application owners should plan to securely enable cloud adoption by developing a security architecture that spans from data center to cloud, providing the same high level of security and threat prevention and extending their existing security policies regardless of location.

Senior business leaders should stay apprised of both the business benefits and the risks associated with their public cloud strategy. This is done by establishing clear communication channels from IT, application owners, security teams to executive management and the board. Periodic reviews should be established that answer many of the questions outlined above so all parties can agree on acceptable levels of risk and understand ho

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com