OPEN DATA CENTER ALLIANCE SM
Security and Privacy Position Paper

Table of contents

LEGAL NOTICE

OPEN DATA CENTER ALLIANCE SM: Security and Privacy Position Paper

Organizations looking to utilize cloud computing services, such as IaaS, SaaS, PaaS, public cloud services or private cloud services, need tools to understand and prepare for security and privacy threats.

There are numerous recent reports regarding specific anecdotal threats, and many people seeking cloud services express particular concern about these intrusions.

ODCA takes a more global, long-term view of security. The threats to corporate and governmental data *are* increasing—and increasingly sophisticated. However, high profile, newsworthy items should not be the focus of an organization's security posture.

Mitigate common vectors

Rather than concentrating on a particular motivation for attack or source, ODCA recommends that organizations focus on the vectors of attack. Attacks are inevitable and constant. While the actors may change, the points that they assault tend to be the same. Fortunately, technology, techniques, and research are available to help in the defense of the organization's assets.

Specific security and privacy requirements vary for each business, in each geographic zone, and under each set of governmental regulations. The threats to the data center are, in fact, not that different for a cloud computing scenario. Black hat actors are still looking to acquire credentials or find flaws in the code of an application whether it is hosted in a private data center or in a shared location.

Research provides organizations with directives that can focus their security attention. Verizon has published the annual Data Breach Investigation Report for the last ten years. This year's Verizon Report identified that 92% of all breaches fell under nine categories.[i]

Similarly, the Australian Signals Directorate (ASD) identified that by adhering to the top four mitigation strategies of their list of 35, an organization can mitigate 85% of threats.[ii] Based on budget, sensitivity to risk, and regulatory requirements, an organization can devise a security posture with an understanding of risk.

ODCA recommends that organizations evaluate their assets, both cloud and otherwise, and understand the threats to each.

Cloud-specific security challenges

While the threats are essentially the same for assets placed in the cloud, risk management and response requires additional steps. Including vendors and partners adds complexity to risk management. As new services and cloud offerings emerge, security controls may not have matured to catch up with the new models.

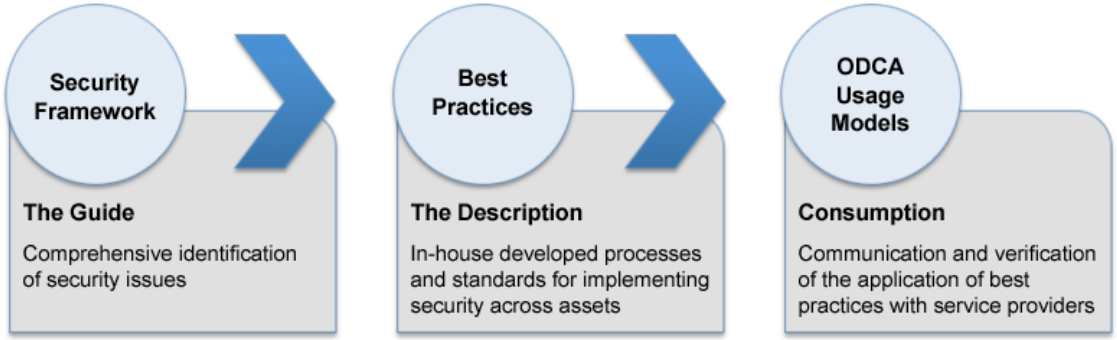
From ODCA's perspective, cloud service providers' responsibility to their customers extends to security. Each vendor needs to fulfill its customer's risk management requirements. The vendor and customer need to discuss ownership and responsibility across all relevant security controls.

Security from the start

Customers have a responsibility as well. As organizations move toward cloud computing they need to communicate their standards and expectations in a way that is clear, consistent, and can be referenced throughout the engagement.

Achieving the vision: framework, best practice, and usage model

Whether public, private, or hybrid cloud computing, ODCA recommends that organizations utilize security frameworks, best practices, and ODCA Usage Models to integrate cloud services into their risk management program.



ODCA recommends that security frameworks inform best practices that are in turn communicated via Usage Models.

Security Frameworks

Existing security frameworks provide the guide for a security position. Each organization's security requirements are different. Companies should seek out a suitable framework based on industry, geography, and regulatory requirements.

Four Commonly Applied Security Frameworks

- The US National Institute of Standards and Technology (NiST) Develops the NiST Cybersecurity Framework (http://www.nist.gov/cyberframework/) for United States Federal Agencies. It is frequently adopted by private organizations.
- In conjunction with a consortium of corporations, the UK government developed the Cyber Essentials Scheme (https://www.gov.uk/government/publications/cyber-essentials-scheme-overview). It is designed to help organizations protect themselves against common cyber attacks.
- The Australian Signals Directorate maintains the Strategies to Mitigate Targeted Cyber Intrusions (http://www.asd.gov.au/infosec/top35mitigationstrategies.htm), 35 strategies that address most threat vectors.
- The Cloud Security Alliance has maintained the Security Guidance for Critical Areas of Focus in Cloud Computing (https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/) since 2009. This framework is specifically designed to help organizations implement security controls for cloud implementations.

Best Practices

A framework will guide prioritization and assist in selecting the proper areas of focus. In those areas of focus, your staff and consultant experts need to develop and document specific best practices for both the customer and the cloud service provider.

Usage Models

In order to guide the consumption of these best practices, ODCA has developed Usage Models. Designed to aid the planning and purchasing options of ODCA members, Usage Models document organizational needs. Those developed by the ODCA Security Workgroup focus on thoroughly expressing security requirements for enterprise cloud computing.

ODCA recommends utilizing Usage Models for specific best practices to communicate with service providers. Verify capabilities against the relevant scenarios included in each usage model. As of June 2014, ODCA has released nine Usage Models. By starting with the Provider Assurance usage model, an organization can help to establish methods to communicate with cloud service providers about security issues.

Assurance Level				
	Bronze	**Silver**	**Gold**	**Platinum**
Description	Represents the lower-end corporate security requirement and may equate to a higher level for a small to medium business customer	Represents a standard level of corporate security likely to be evident in many enterprises	Represents an improved level of security that would normally be associated with the processing of sensitive corporate data	Represents the highest level of contemplated corporate requirements
Example	Development environment	Test environment; "out-of-the-box" production environment	Finance sector production environment	Special purpose, high-end security requirement

ODCA Usage Models utilize these four categories of assurance levels to identify the security posture suited to the customer needs.

An ongoing commitment

Security does not stop at the RFP or when the system goes live. As the threats evolve, risk management must be an ongoing process of awareness and response. Allocate appropriate resources and confirm that service providers have also assigned staff time to performing security tasks.

Conclusion

There will continue to be cyber threats for the IT organization, and we can be confident that those threats will grow in sophistication. Instead of focusing on the sources of these threats, ODCA recommends that organizations apply a consistent process and develop security risk management that incorporates their cloud service providers and cloud technologies.

Best Practices From ODCA

- Select and utilize a cyber security framework that best applies to your organization.
- Leverage ODCA Security Usage Models when planning your data center, or private or public cloud engagements.
- Think security from the start; implement the specific directives within the ODCA Security Usage Models when planning and selecting cloud computing solutions.
- Follow all regulations relevant to your industry.

[i] http://www.verizonenterprise.com/DBIR/
[ii] http://www.asd.gov.au/infosec/top35mitigationstrategies.htm