White Paper

Cloud Security Implications for Financial Services

avanade

Introduction

Growing Adoption of the Public Cloud

Businesses in nearly every industry are rapidly adopting cloud computing as a vital part of their IT operations and a path to divesting their expenditures in server hardware by 2020. With greater flexibility, ease of upgrade, and low capital investment requirements, the public cloud makes it easier for organizations to implement newer, more competitive computing tools, like mobile solutions, real-time data analysis, and the latest application innovations. In addition, organizations that have inherited legacy systems through acquisition have found moving to the cloud to be more cost-effective and more secure than keeping older systems up-to-date. As a result, while the financial services industry is still in the early stages of moving to the cloud, most organizations do have a cloud strategy, usually a mix of on-premises (on-prem), private, and public cloud infrastructure.

Fear, uncertainty, and doubt, however, continue to plague financial organizations looking to make the move to the public cloud. While some financial services firms continue to maintain an on-prem or private cloud only approach, due to security and compliance concerns, overall confidence in the public cloud has been rapidly growing. Continuous security improvement in the public cloud has driven more businesses to migrate their processes to the public cloud to gain a cost and operational advantage over their competitors. Furthermore, public cloud service providers are rapidly meeting global compliance requirements, making a move to the public cloud a more secure decision.

Moreover, with the public cloud's economies of scale, protections built to meet the needs of one constituency become part of the of the shared platform. For example, for multiple companies sharing cloud server space for their email functions, when "malware" is found in an attachment from one tenant, it can be tagged and prevented from affecting other tenants sharing the compute resource. In the public cloud, there is an opportunity for "community" benefit through shared innovation, security upgrades, and lessons learned.

Problem: Public Cloud Security and Compliance

The questions many financial services organizations face when considering moving to the cloud are: *Will the public cloud be secure enough for my operations?* and *Can the public cloud meet my worldwide compliance requirements?*

There are no regulations that prevent financial services organizations from moving to the cloud, and, in fact, there are cloud solutions that help companies meet regulatory requirements. For example, Microsoft Azure is compliant across many financial regulations to include Center for Financial Industry Information Systems (FISC), Payment Card Industry Data Security Standards (PCI DSS), and Service Organization Controls (SOC) 1, 2 and 3.

Microsoft has leveraged its decades-long experience in enterprise software to build a secure public cloud platform. Microsoft Azure has gone through security hardening by continuously improving security-aware software development, operational management, and threat-mitigation practices that are essential to the strong protection of services and data. A public cloud solution, like Microsoft Azure, can be more secure than private cloud or on-prem installations.

Security in the public cloud is a shared responsibility and follows a shared security model, which means clients have an important role to play in public cloud security. While Microsoft Azure provides security for the overall global cloud infrastructure and foundational services in the public cloud, clients still need to take steps to:

- Secure customer data and content, Azure environment, Azure Accounts, Access Controls and Network Configuration
- Ensure proper configuration of virtual machines to prevent attacks
- Turn on data collection in the Azure Portal to allow logging and monitoring and enable the Intrusion Prevention System (IPS) to defend against network and application threats
- Configure properly the Host Firewall

Microsoft Azure reduces vulnerabilities to breaches in software by implementing the Microsoft Security Development Lifecycle (SDL), a mandatory software security assurance process followed by Microsoft and its partners. Microsoft also follows the Microsoft Operations Security Assurance (OSA) framework to manage risk in online and cloud services, and implements security controls from both the National Institute of Standards and Technology (NIST) 800-53 and International Standards Organization (ISO) 27001:2013.

Shared Security Model

While Microsoft Azure secures an organization's overall global cloud infrastructure and foundational services in the public cloud (see sections in blue in the chart below), clients will need to secure their customer data and content, Azure environment, Azure Accounts, Access Controls, and Network Configuration. Clients will also need to ensure the proper configuration of virtual machines to prevent attacks. In addition, to defend against network and application threats, clients must make sure that data collection is turned on in the Azure Portal to allow logging and monitoring to take place, as well as ensuring that Intrusion Prevention System (IPS) & the Host Firewall are property configured.

This is where Avanade Managed Services (AMS) comes into to play. Avanade has the deep Microsoft technology stack expertise to help clients configure Active Directory Federated Services in the cloud, Azure Rights Management Services (RMS), as well as network, firewall and client side and service side encryption.

Avanade also offers the Microsoft Azure "community" benefit that comes with having clients with more stringent security requirements than most other companies. Over the last few years, major cloud service providers have implemented significant security improvements that create a common denominator effect that benefits all clients looking to move to the public cloud platform. Also, cloud security partners – such as Avanade – provide additional managed security solutions and services on public cloud platforms such as Azure, such as the latest security technologies and security as a Service (SaaS) offerings.

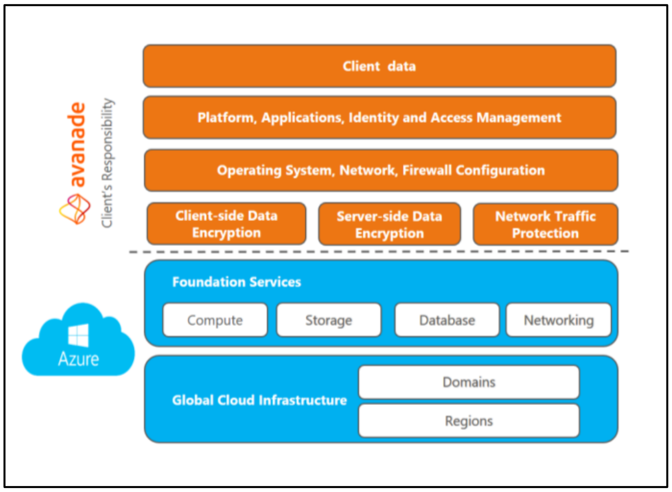
avanade
Client's Responsibility
Client data
Platform, Applications, Identity and Access Management
Operating System, Network, Firewall Configuration
Client-side Data Encryption
Server-side Data Encryption
Network Traffic Protection
Azure
Foundation Services
Compute
Storage
Database
Networking
Global Cloud Infrastructure
Domains
Regions

Figure 1-Shared Security Model

Regulations Impacting Financial Services

Financial services regulations address a wide range of concerns, including privacy, disclosure, fraud prevention, anti-money laundering, anti-terrorism, anti-usury lending and anti-lending discrimination. It is a complex landscape due to the number of institutions around the world that financial services regulations, especially in the U.S., where laws are put in place not only by the federal government, but also at the state and city levels.

Primary Regulations That Impact Financial Services Companies

Country	Regulation	Areas covered/requirements	Cloud security considerations
U.S.	Payment Card Industry Data Security Standards (PCI DSS)	All organizations that accept, acquire, transmit, process or store cardholder data must safeguard all sensitive customer information.	Verify that contracts are well-written, expectations are set, and nested 3rd-party relationships (sub-vendors) are identified and made aware of their obligations.
U.S.	Sarbanes-Oxley (SOX)	Accountability for financial reporting and governance; quick reporting of compromised sensitive data	Implement controls to protect in-scope data (such as encryption for data at rest); access controls, decryption for only those authorized to see financial information, monitoring logs, and validated incident response processes.
U.S.	Gramm-Leach-Bliley Act (GLB, GLBA, or the Financial Services Modernization Act)	Applies to US financial institutions and governs the handling of non-public personal information (customer financial records and other personal information).	

Other Regulations and Guidelines to be Aware Of

Country	Regulation	Areas Covered/Requirements
U.S.	Federal Deposit Insurance Act – section 36	“Early Identification of Needed Improvements in Financial Management”
U.S.	National Credit Union Administration rules and regulations	Include the Federal Credit Union Act which governs the coverage and terms of insured accounts at all federally insured credit unions
U.S.	Patriot Act	Section 311: Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern
U.S.	Regulation P (1999)	Financial institutions must inform a consumer of their policy regarding personal information and must provide an "opt-out" before disclosing data to a non-affiliated third party.
U.S.	“Know your customers” rules and Bank Secrecy Act (1970)	Financial institutions must ensure customer financial activities are consistent with their business activities, and report suspect activities to the government.
U.S.	State data breach notification laws	California enacted the first in 2003, and now there are 47 states, as well as Puerto Rico, Guam, and the Virgin Islands, that have passed their own data breach notification requirements. California and other states define personal information to include email addresses and passwords.
U.K.	UK Data Protection Act	Data breach disclosure law
Japan	Financial instrument and Exchange Act (Japan) – JSOX	Rules for internal controls related to financial reporting
Korea	Personal Information Protection Act	Data breach disclosure law

Other Regulations and Guidelines to be Aware Of

Country	Regulation	Areas Covered/Requirements
Australia	Privacy Amendment (Notifiable Data Breaches) Act 2016 Amends the Privacy Act of 1988 and takes effect on February 22, 2018	Data breach disclosure law requires a company to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of certain data breaches that are “likely” to result in “serious harm.”
Hong Kong	Hong Kong Monetary Authroity (HKMA)	Provides guideines for: • Data security (Personal Data Privacy Ordinance [PDPO]) • Incident handling and reporting • Cybersecurity (“Cybersecurity Fortification Initiative” [CFI])
Singapore	Monetary Authority of Singapore (MAS)	Provides guidelines: • Notify MAS of security breaches • Assess and regularly audit 3rd-party service providers • Ensure cloud service provider: (1) can clearly identify and segregate customer data; and (2) has robust access controls to protect customer information

Security Vulnerabilities in the Financial Services Industry

In 2016, the financial services industry reported a total of 33 data breaches, impacting over 1 million records. Security Scorecard, a cybersecurity and risk monitoring platform, noted that as financial institutions have grown through acquisition, they also have inherited legacy IT systems with vulnerabilities that remain in place for years.

In its 2016 report, Security Scorecard found that[1]:

- The U.S. Commercial bank with the lowest security posture is one of the top 10 largest financial service organizations in the U.S (by revenue).
- Only one of the top 10 largest banks received an overall 'A' grade.
- Ninety-five percent of the top 20 U.S. commercial banks (by revenue) have a network security grade of 'C' or below.
- Seventy-five percent of the top 20 U.S. commercial banks (by revenue) are infected with malware.
- Nearly 1 out of 5 financial institutions use an email service provider with severe security vulnerabilities.

Security Scorecard looked at 361 companies that had experienced security breaches in 2015-2016. Of those, more than 10% represented the financial services industry, where common areas of vulnerability were network security, due to challenges in auditing and updating large infrastructures, and timely security patches, usually required by legacy systems no longer supported by application providers. leading target of cybercriminals. Unpatched systems have been a popular target for cybercriminals.

Some of the Largest Data Breaches to Impact the Financial Services Industry:			
Year	**Operation**	**Event**	**Estimated total loss**
2016	Asian central bank	Cybercriminals installed credential-stealing malware to obtain log-in credentials to the Society for Worldwide Interbank Financial Telecommunications (SWIFT) Network.	$81 million
2014	Major U.S. bank	A cyber-attack compromised the financial and personal information of 76 million households and 7 million small businesses.	$1 billion (Protection Group International's estimate of total related costs)
2012	Leading retail payment technology company	A cyber-attack on the company's North American servers enabled criminals to steal personal data from 1.5 million credit card accounts.	$90 million

[1] http://www.prnewswire.com/news-releases/americas-financial-industry-highly-susceptible-to-data-breaches-300307516.html ; http://info.securityscorecard.com/2016-financial-cybersecurity-report

Maintaining Data Security and Regulatory Compliance

Because of the number of regulations affecting the industry, as well as the volume of personal information and money involved, maintaining data privacy, security and compliance is a major responsibility for financial services organizations. There are, however, effective steps that organizations can take to protect their systems and data – both on-premises and in the cloud – as well as operate within the law:

Data Challenge	Mitigation Approach
Security	• Data encryption of the appropriate strength for the sensitivity of the data it looks to protect against data loss and/or theft • Consider Scenarios for ○ Data in transit ○ Data at rest • ISO 27002 and the NIST 800 series I frameworks • Penetration testing and regular key control validations • Online account access 2-factor authentication
Early detection (of unusual activity or unauthorized data access)	• Security Event and Incident Management(SEIM) system with audit trail capabilities that record and analyze instances of different categories of data accessed (what, when and who) and changes to information • Incident Response processes (people and governance) • Forensics capabilities (technical analysis of reviewing evidence of a potential data breach)
System vulnerability	• Risk analysis/assessment with regular review and system audits • Routine audits of user access (continued need for access rights) • Security and Privacy by Design when developing new systems (SDLC, tollgates/milestone validations) • Regularly recurring penetration testing and code review for top systems (existing systems) • Map and Inventory Data (collection point, storage locations and transfer to upstream and downstream systems)
Human error	Employee training (to prevent gossip, unintentional data disclosures, loss, deviation from standard procedures, phishing and social engineering)

Avanade's Approach to Security and Compliance

Avanade understands that financial services companies have a lot to consider when moving to the cloud. With in-depth experience providing a variety of cloud solutions, Avanade helps organizations realize the benefits of these programs – all while protecting data and maintaining compliance. Moreover, working with its partners, Accenture and Microsoft, Avanade offers an unmatched combination of industry and technical expertise. In fact, one cloud service platform that is a great fit for financial services companies is Microsoft Azure, designed to meet high security standards. Avanade is a Microsoft Gold Certified Azure Partner.

Avanade helps organizations move their IT operations to the cloud through migration, implementation and managed services, investing time to fully understand each client's unique requirements. The company assigns every client engagement to the company's **Client Data Protection (CDP) program**, built upon the following principles:

- **Senior-level oversight** responsibility for all engagements where client data is accessible
- **Clear communication and documentation** of all CDP requirements
- **Establishment of a business associate agreement (BAA)** to allow proper handling of all client Personally Identifiable Information (PII)
- **Mandatory CDP HIPAA awareness training** for all resources tasked with maintaining any aspect of a client solution, in addition to training specific to the individual client requirements
- **Required controls** for secure handling of client data while in Avanade's custody
- **Service-specific controls** tied to vulnerabilities inherent to unique types of work, such as the needs of financial services clients
- **Technology controls** deployed to enforce mandatory baseline protection mechanisms
- **Tools, processes and subject matter specialist support** for project teams
- **Standardized data protection** tools and templates

Program execution begins with a risk assessment to determine each client's risk in relation to their precise project requirements. The second mitigation phase uses an implementation plan consisting of up to 24 control families operated by the project team.

Avanade requires that a CDP plan must be established before any service delivery tasks begin, and client stakeholders, such as business owners and representatives from the Information Security team, and the Avanade service delivery team must adhere to the plan for the life of the engagement. Plan execution is periodically reviewed by independent internal teams to gauge both compliance and the effectiveness of the controls to manage the client's risk. Any identified gaps are tracked and escalated to the assigned Client Data Protection Executive (CDPE) for corrective action.

Avanade's knowledge of financial services regulations around the world – and its experience helping clients protect their systems and information – have enabled the company to create a library of best-practices and effective approaches to security. Avanade knows, however, that every client is different, and each has its own set of requirements and challenges. That is why Avanade makes sure it understands these elements during the assessment process so that the company can develop and put in place the right security controls to fit a client's individual needs. Moreover, Avanade continues to reassess those needs throughout delivery, ensuring that the company provides services that its clients can count on to help keep data safe, systems protected, and their organizations regulatory compliant.

About Avanade
Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation and has 30,000 professionals in 24 countries.
Visit us at www.avanade.com

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Africa
Pretoria
Phone +27 12 622 4400
SouthAfrica@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
Asia-Pacific@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com