Table of Contents

I. Introduction: Security challenges in regulated industries...........................................1
II. Cloud adoption rates by industries................................................................................1
   Healthcare.........................................................................................................................1
   Finance.............................................................................................................................2
   Government.....................................................................................................................3
III. Regulated cloud initiatives of 2015.............................................................................4
   File storage, sharing and collaboration........................................................................4
   CRM..................................................................................................................................4
   Remote Access...............................................................................................................4
   Mobile Data Transfer.....................................................................................................5
IV. Data Security Best Practices........................................................................................5
   Client-vendor agreement..............................................................................................5
   HIPAA and HITECH Compliance in Healthcare.........................................................5
   Educating the Employees.............................................................................................6
V. Conclusions......................................................................................................................6
References............................................................................................................................7
Executive Summary

Modern organizations need powerful computing solutions to effectively manage communications and securely store their data. Emerging as a cost-effective way to modernize IT infrastructure, cloud computing has been one of the most important technology trends over the last few years. Businesses of different sizes recognized its potential and started working with cloud vendors on moving specific workloads to public servers. However, even though the cloud is no longer new technology, multiple security issues are still associated with its implementation. These remain a major inhibitor for more sectors to adopt cloud solutions, which is particularly the case with the institutions that operate in regulated industries and need to follow specific rules on data storage and transfer. Over the last few years, however, vendors have increased their focus on security and started delivering more stable solutions, which enabled organizations in regulated industries to increase their use of the cloud.

I. Introduction:

Security challenges in regulated industries

Compared to most other sectors, the organizations that operate in regulated industries were slow to adopt cloud computing solutions and move their workloads to public servers. This is mainly due to the challenges associated with data protection and risk management, which are particularly important given the high sensitivity of data these organizations work with. Unsurprisingly, the government, healthcare and finance industries hesitated to introduce cloud as a form of IT innovation and simplify their mission-critical processes. The most important concerns certainly relate to considerable threats that the public cloud may bring, as well as the misconceptions of shared responsibility between organizations and vendors.

Such concerns have been dominant in the regulated industries ever since the rapid IT modernization with the cloud has started and are still relevant for both client organizations and vendors themselves. While the former increasingly explore the cloud’s flexibility and the ways to maintain maximum data security, the latter strengthen their focus on delivering more stable solutions. Therefore, both sides seem to have recognized data security as the major inhibitor to a wider cloud adoption in regulated industries, which has brought about a growing diversity of secure solutions.

With an aim of examining cloud data security best practices for the regulated industries, this white paper will examine the current cloud adoption rates, as well as the offering of solutions designed to provide the necessary level of data security.

II. Cloud adoption rates by industries

Healthcare

Like most other industries reliant on service operations, healthcare is gradually shifting to cloud computing in order to lower IT costs and improve the efficiency of their processes. Despite the implied implementation challenges and security concerns, recent surveys suggest that the industry representatives are aware of the cloud’s potential and consider the realization of the migration process indispensable.

Today, an average healthcare institution uses 928 cloud services, which speaks about the popularity of this technology. However, only 7.0% of these solutions actually meet the necessary security standards and most are still unknown to IT administrators, as confirmed in Skyhigh’s report on Cloud Adoption & Risk in Healthcare. In relation to the use of the cloud, the survey also reveals that the average organization uploads 6.8 terabytes to the cloud each month, while healthcare practitioners use as many as 26 cloud applications on a regular basis. Such an increased reliance on the cloud could expand vulnerability of the entire organization, which is an alarming fact considering the value of healthcare information.
Namely, a healthcare record is estimated to be 20 times more valuable than stolen credit card information and this is the main reason why cyber criminals often use consumer cloud apps to obtain sensitive information from healthcare practitioners’ accounts. Therefore, by using high-risk cloud services, employees themselves bring patients’ and researchers’ data at risk, thus contributing to the increased exposure of the whole sector to compromised accounts.

**Finance**

As further outlined in the SkyHigh report, finance is the industry with the largest exposure to insider threats based on the number of employees who reported having at least one credential stolen.

![% of employees with at least one stolen password](skyhigh_skyhigh_report)

Compared to any other industry, **finance institutions suffer 300% more cyber-attacks** and are justifiably concerned about the security of their data. Unsurprisingly, out of all the regulated industries, the lowest response regarding cloud computing implementation was in finance.

Here, the question of control and responsibility remains a difficult one, offering very few acceptable solutions this far. However, parallel to the advancements in technology, the number of finance institutions embracing the cloud also grew rapidly. The survey conducted by the Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector* suggests that the adoption rates are particularly high in larger companies (500-5000 employees), even though the threat awareness still exists. Most respondents cited the following as their main cloud security concerns:

- Security concerns: 86%
- Compliance concerns: 86%
- Privacy: 79%
- Data retention and destruction: 79%
- Data residency: 75%

To overcome these challenges, IT administrators opt for different combinations of private and public clouds, while some continue to insist on a strict no-cloud policy. The graphic below illustrates some of the most commonly used cloud-related policies to handle data security in the finance industry.

![Cloud strategy - companies are approaching their cloud strategy](cloud_security_alliance_report)
Government
The pace at which federal enterprises and government agencies are adopting the cloud solutions is similar to that in healthcare and finance. Although the official initiatives regarding the cloud computing adoption were set several years ago, its benefits are still widely discussed by the officials in the US and beyond. As concluded at Oracle OpenWorld panel in October, 2015, government agencies still see the cloud as the best form of IT modernization available. Among the US government officials who addressed the issue, Congressman Will Hurd, 23rd district Texas, reminded that the government keeps flushing significant resources to outdated systems instead of building secure infrastructure in the cloud. In a CIO interview, the congressmen insisted on the urgency of the matter, explaining that the systems that are currently in use are not only inefficient, but unreliable as well.

“Legacy systems are expensive to maintain and often make sensitive information vulnerable to cyberattacks. The Labor Department has a 30-year-old system developed by people who are now all dead. They had to resort to looking for old parts on eBay.” - Will Hurd

However, this sector also sees data security management as a major challenge for not only government agencies, but other organizations, as well. To ensure safe cloud migrations, congresswoman Nikki Tsongas of the 3rd congressional district Massachusetts introduced the Department of Defense Cloud Security Act, requesting a full evaluation of IT security and cloud implementation requirements. The legislation was aimed at encouraging secure cloud implementations and enabling both government and commercial organizations to safely operate with their data.

“The DoD must more effectively take advantage of technological advancements, such as cloud technology, but do so in a safe, efficient way. This legislation will allow DoD to take full advantage of the cloud services and best practices from both the government and commercial sector, which will, in turn, decrease costs, increase accessibility and allow for a more secure system overall.” - Nikki Tsongas

Apparently, the government industry recognizes the need for efficiency, agility and innovation and is more open to finding the way to make the best of the available technologies. With the current cost of IT maintenance in the industry rising as high as $80 billion annually, the significantly smaller amount of $20 billion is needed for maintaining the same services using cloud computing solutions. Therefore, it is unsurprising that US state officials more frequently discuss the benefits of the cloud, with Congressman Hurd and Congresswoman Tsongas being some of the most vocal ones.

In addition to them, an important government cloud initiative was presented in Wyoming, which was the first state to implement Google Apps for Government in 2011. The government thus set the example for all the other US states, especially since their focus on the cloud continued. As suggested in the mission statement of the Department of Enterprise Technology Services, Wyoming, the cloud represents an important focus within the strategy for delivering tech potential to business innovators. Namely, the government plans to integrate the cloud across different sectors and enable large-scale IT innovation that meets security standards. In relation to this, staff engineer Courtney Thompson of ETS pointed out that their cloud data is well protected, whereupon vendor agreement on accountability is one of the key factors of successful migration.
These initiatives, coupled with the advancements in technology itself, contribute to raising awareness of the cloud’s potential and encouraging the leading vendors to increase their focus on security. The results, especially in 2015, have been reflected in the greater offering of tools and platforms designed specifically for the needs of regulated industries.

III. Regulated cloud initiatives of 2015

The year 2015 has seen some major releases aimed at facilitating data security management in regulated industries. Among the leading tech providers, IBM, Salesforce and Box all released regulated industry solutions, which marked a significant shift in their focus. Together with the existing vendors that have been delivering solutions compliant with the national regulations for years, such initiatives help in creating more options for the organizations in regulated industries globally. Considering the fact that all these providers cater to businesses and enterprises, these steps are not at all surprising. Namely, according to Markets and Markets report, the cloud security market is predicted to reach $8.71 billion by 2019, bringing significant opportunities for vendors.

Evidently, the demand for secure solutions is only to further grow in the next few years, thus making additional pressure for vendors to deliver stable storage and communication solutions. Among those currently in use, the following represent reliable ways for organizations in regulated industries to control the use of cloud applications and improve the overall security of their data.

**File storage, sharing and collaboration**

In September, 2015 Box released Box Governance to allow end-users to organize their business life cycle from the very creation to regular maintenance and eventual disposition. The platform provides the ability to set automated policies and have a constant insight on protection and removal of the organization’s data. Additionally, it prevents certain downloads and enables monitoring of the uploaded data to prevent potentially risky transfer of sensitive information.

**CRM**

An established magnate in the field of CRM, Salesforce created an advanced solution in the field of Customer Relationship Management aimed at the healthcare industry. Salesforce Shield is an advanced platform that provides secure connections between doctors, practitioners and patients to allow easier transfer of sensitive information. It also offers visual data representation for every connection, helping the comprehension of a certain patient condition, action and satisfaction, or relationship flow.

**Remote Access**

SecureLink Remote Access Solution allows technology vendors to monitor and manage third-party connections. A safe, HIPAA-compliant and constantly audited connection provides user-friendly and protected correlations between vendors and consumers, satisfying the needs of both. All third-party admissions are predetermined in accordance to users’ preferences and rules of access, through a user-friendly browser interface. A two-factor authentication verifies approved access and, with the help of high-definition audit, every entry is recorded and presented at request in complete transparency. This solution practically eliminates the risk of shared accounts and credentials.
Mobile Data Transfer
A leader and innovator in the field of data storage, IBM launched a secure solution aimed to help organizations manage shadow IT and monitor employee’s use of mobile apps. Cloud Security Enforcer provides a full and detailed report on any inquiry regarding company file transfers, with generated reports through a simplified service. All access control is under the management of the user; audit includes a thorough report of transfer activity and transaction, as well as the policy enforcement with license key management. In addition to the vendors outlined above, a variety of other companies currently works on high-security systems adjusted to the use in organizations that operate with large volumes of sensitive data. In such settings, deploying only the most reliable solutions is a key to IT modernization and the first step to improving the overall data security.

IV. Data Security Best Practices

Client-vendor agreement
The deployment of cloud computing systems in individual organizations should primarily rest upon the right choice of a vendor. While most organizations decide to build their own private clouds to ensure maximum security for their most valuable data, employees’ communication and collaboration needs increasingly require flexible cloud solutions. This is why organizations need to find the right ways to monitor their employees’ use of high risk applications, which is why they often need to implement external IT components. This means that most organizations are required to operate in a hybrid cloud environment in order to meet both performance and security standards. Here, the key for successful collaboration is the creation of a comprehensive SLA that is crafted in such a way to enable quick disaster recovery, precisely outlining responsibilities of both clients and vendors. In their guide to secure cloud implementations, CSA outlines a set of steps recommended for efficient creation of cloud SLA in regulated industries:

• Connect legal and IT teams to assess a vendor’s standard terms and create an agreement tailored to the individual organization.
• Analyze current compliance requirements, as well as the compliance scope to eliminate the possibilities of being impacted by international regulations under which the vendor operates.
• Understand the responsibilities of each party when it comes to activity reporting, logging, data retention, incident response, controls testing, and privacy policies, and whether these aspects might change at a certain point.
• Collect evidence of how each requirement is met to provide the necessary information for consumers and partners.

HIPAA and HITECH Compliance in Healthcare
In order to ensure maximum security of data records and provide the necessary privacy for patients and researchers, US healthcare institutions need to comply with HIPAA and HITECH regulation acts when implementing new technologies. So far, most cloud providers were unable to provide the necessary level of security under these regulations, which was highly limiting for healthcare institutions. Over the last few months, however, the offering of solutions that directly address these issues increased. Namely, a greater number of vendors have developed secure solutions for regulated industries, which contributed to the wider implementation of the cloud.
Educating the employees
While the use of advanced security systems by reliable vendors represents the key to maximizing cloud data security, employees’ awareness on the best security practices is an important factor of the overall stability. As discussed above, the employees’ use of high-risk cloud apps for sensitive data transfer increases the vulnerability of the whole organization, which is why it needs to be addressed separately. Besides regulating data access and authorization, organizations need to ensure all of their employees understand and are ready to follow the recommended practices for secure data storage, transfer and management. This refers to the information sharing across different online accounts, as well as personal cloud services. Introducing secure passwords and recommended username-password conventions is one way for CIOs to ensure all the employees are putting the theory into practice whenever managing the organization’s documents.

V. Conclusions
The apparent change in attitudes towards the cloud adoption in regulated industries is influenced by different factors, the most important one being a greater availability of solutions designed to meet the highest security standards. Given that finance, government and healthcare previously had a limited set of solutions that meet compliance requirements at their disposal; it is unsurprising that it took years until they embraced the new technology. Today, the cloud is in a more mature phase, allowing vendors to better use its potential and create solutions for organizations that operate with highly sensitive information. Such possibilities are a key driver of growth of the cloud in regulated industries and provide more opportunities for global finance, healthcare and government industries to reinvent their IT processes. The next generation solutions, however, are certainly not the only factor of that contributes to safer cloud data management and there are still numerous issues that need to be addressed before workloads are moved to public servers. Finding a solution for these issues is precisely what may make a huge difference in the way cloud data will be managed in regulated industries in future.
References:


Department of Enterprise Technology Services. Wyoming.
http://ets.wyo.gov/

Exploring the Cloud: A Global Study of Governments’ Adoption of the Cloud. Kpmg.com


https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

http://www.cloud-council.org/cscchealthcare110512.pdf

For more information visit securelink.com.