Cyber in the Cloud

Lessons Learned from Idaho National Laboratory's Cloud E-mail Acquisition

Troy Hiltbrand, Idaho National Laboratory
Daniel Jones, Idaho National Laboratory

Abstract. As we look at the cyber security ecosystem, are we planning to fight the battle in the same way we did yesterday, with firewalls and Intrusion Detection Systems (IDS), or are we sensing a change in how security is evolving and planning accordingly? With the technology enablement and possible financial benefits of cloud computing, the traditional tools for establishing and maintaining our cyber security ecosystems are being dramatically altered and organizations need a way to effectively manage this transition.

During World War II, the Japanese took possession of U.S. soil only once. For a short period of time, they occupied the tiny islands of Attu and Kiska, off of the Alaskan coast [1, 2]. In response to this occupation, U.S. and Canadian forces fought hard and succeeded in reclaiming Attu, but not without heavy casualties. Coming off of this ordeal, these same forces stormed Kiska armed with the knowledge that they had earned through blood, sweat, and tears, anticipating that conditions would be nearly identical due to the similarity in the islands. Upon securing the island of Kiska, they learned that their efforts been in vain. The Japanese had changed tactics and had slipped through the Navy blockade surrounding the island under the cover of fog and had escaped instead of fighting a losing battle. This did not mean that the fight for Kiska went over flawlessly. In fact, there were casualties due to friendly fire. From this, we can learn a great lesson about the nature of battles and their ever-evolving nature. Just because we understand what has happened in the fight to this point does not mean that we are completely prepared for the fight ahead.

As we look at the cyber security ecosystem, are we planning to fight the battle in the same way we did yesterday, with firewalls and IDS, or are we sensing a change in how security is evolving and planning accordingly? With the technology enablement and possible financial benefits of cloud computing, the traditional tools for establishing and maintaining our cyber security ecosystems are being dramatically altered.

For this purpose, we need to migrate our thinking from an incident-response model, in which we put in place controls and safeguards against threats based on historical activity to a risk management framework, where we assess our greatest risks areas and apply our resources and efforts towards only those risks which demand the most attention.

Additionally, the cyber security domain has been the purview of engineers and technologists. As cloud computing services are deployed, organizational technical personnel will no longer be the sole provider of security controls and incident response. The primary functional domains of cyber security, in the cloud, will be mission/business, legal, and contractual. Technology will remain a critical functional domain, but for many organizations this responsibility will be transferred to the cloud service provider or a joint responsibility.

Recently, Idaho National Laboratory (INL) participated in a push to move e-mail services to the cloud and through this activity has identified some mechanisms that can help facilitate ensuring cyber security in the cloud.

Risk Management Framework

In the past, we have had physical and logical controls over all of the layers in our computing environment and so we were relatively confident that we could defend all of the resources equally well. No longer are we able to put up the fortifications around our network boundaries and treat all of our informational assets equivalently within that boundary. Cyber security exists to protect those information assets of highest value to the organization. As we move towards a cloud model, our control changes and we have to identify both how to best protect those resources with the highest value and identify which resources are and are not candidate to move into a cloud, which is beyond our physical control. To do this, it is first important to understand which organizational resources are candidates to be hosted in a cloud model. The historical "peanut butter spread" approach is not financially sustainable.

Mission/Business Context

The first step in assessing what assets are candidate to move into the cloud is to evaluate the impact of the move in the following areas:

1. Mission/business benefits and impacts
2. Legal analysis
3. Financial analysis
4. Human/cultural impact
5. Technical cyber security review

Within each of these categories, the organization assesses whether the risk profile is affected in a positive or negative manner and to what extent that impact occurs.

Mission/Business Benefits

Technological decisions cannot and should not be made independent of the mission or business. All technology decisions are ultimately business decisions and require that the mission-related benefits be factored into the overall risk assessment. Moving to the cloud can help enhance or hinder mobility, accessibility, flexibility and agility and needs to be assessed to determine if the movement to the cloud assists or precludes the business from achieving its mission.

At INL, one of the major drivers on the horizon is the ability to collaborate and communicate with external partners in the performance of research and development activities, including foreign partners. The use of collaboration in the cloud positions us to meet the business needs for the future.

Legal Analysis

Organizations are legal entities and are bound by Governance, Regulatory and Compliance (GRC) requirements, including:

- Export Control
- eDiscovery
- Information ownership and use rights

Export control entails protection and control of specific information from leaving the boundaries of where it is created. As information moves to the cloud, is it necessary to understand how the risk profile of the information in the cloud change and also the impacts of the organization to control future movement of information. With our acquisition, International Traffic in Arms Regulations (ITAR) information was a significant consideration due to our mission objectives [3].

eDiscovery involves the responsibility of participating in the discovery process and delivering applicable information to a court of law on request. With the tools provided by our cloud provider, we were able to significantly increase our ability as an organization to participate in the discovery process and comply with legal regulations. With the increase of capabilities, the laboratory had to further refine retention policies associated with information. This was to ensure that we were being as protected as possible, while also ensuring that we were maximizing our responsiveness and compliance with GRC requirements.

Information ownership and use rights are also critical. When an organization places information assets in the cloud, ownership and utilization rights to the information have to be addressed, including the rights of the provider to disclose the nature of the relationship to further its own pursuits. The Terms and Conditions and Terms of Service of the contract are the vehicles that establish ownership and utilization along with Federal and State laws.

Financial Analysis

One of the major pushes associated with moving into the cloud is financial. The models associated with the cloud are inherently different from an organization hosting the same solution on premises. The fundamental selling point of cloud computing is that it provides organizations maximum flexibility, especially in terms of incremental investments. With on premises solutions, the financial model requires up-front capital investment to install and configure the solution and then a reduced operational budget over the life of the solution. With the cloud, the up-front acquisition and implementation are reduced, but a greater portion of the total cost of ownership lives as operational costs associated with maintaining the solution.

With cloud solutions, organizations are more agile in their ability to increase or decrease service in small increments based on demand. The extent of this scalability is bound by the nature of the cloud. A cloud with more tenants (e.g. public cloud) is more flexible than one with limited tenants (e.g. private cloud).

At INL, we were moving into the cloud from an organizationally hosted legacy technology that was acquired and implemented during the 1990s. The technology had become outdated and was no longer sustainable and necessitated an upgrade. We opted to adopt the cloud finance model because it allowed demand and supply to be more flexibly matched.

Human Cultural Impact

Although businesses are entities, they are the composite of individuals. It is the cohesion and direction of those individuals under the charge of a defined organizational leadership that makes or breaks an organization. This requires that the impact on the culture for a given solutions needs to be assessed. Understanding whether the move to the cloud will help or hinder individuals from being successful is important. This entails understanding the impact on individual's effectiveness in performing work, attitudes and behaviors towards safety and security, and the perception of their role in security. There is often fear, uncertainty, and doubt among the organization's culture when moving to the cloud because the execution of work changes location and people are uncomfortable with change. This does not automatically exclude the cloud because people are hesitant to change, but the ability to mitigate this risk does need to be assessed. If the organization has the capability and the responsiveness to cultural change, movement to the cloud can be successful. If past efforts have shown that the culture is incapable of making the change, the risk in this area needs to reflect this challenge.

At INL, this has been a significant consideration. We understand that over the next 10 years, a large portion of our workforce will be ready to retire and that the upcoming generation, defined by the Federal CIO as the "Net Generation," [4] will demand working in a much different way than is common in our workplace today. In looking at our current workforce, we have identified that through effective communication and organizational change management, they will be amenable to the change and that it will position us for a more high performance workplace for the future. Balancing the needs of the current workforce and the future workforce has been a significant consideration in the movement of collaboration and communication into the cloud.

Technical Cyber Security Review

When taking any asset into the cloud, it is important to understand the technical impact on other assets. If components of information are moved to the cloud, there is potential for unintended repercussion on other information assets. This is especially critical when information is integrated between systems. If integrated assets are shared between the internal network and the cloud, the overall risk profile of that relationship can potentially increase. The entire scope of the move needs to be understood and the impact to the overall risk profile needs to be assessed.

As INL reviewed the movement of e-mail to the cloud, there were a number of key technical issues that had to be considered. With much of e-mail throughout the laboratory being encrypted in transit, key management was a major consideration in the movement to the cloud. Moving the keys to the cloud did not make sense for the organization, but process had to be established to allow the use of these keys by a service that resides in the cloud. Through the use of OAuth and a security gateway, we were able to preserve complete control of our key management and still be able to administer secure login management to the cloud.

Net Scoring

With each of these areas assessed, we were able to combine to score the direction and relative magnitude of the risk impact to identify the overall risk profile for the organization with respect to moving e-mail into the cloud.

As INL performed the risk assessment of moving e-mail to the cloud, we identified that overall risk profile of our organization improved by moving this particular service into the cloud. Below represents the scoring in this specific assessment:

- Mission benefits (+2)
- Legal impact (0)
- Financial impact (+2)
- Human/cultural impact (+1)
- Technical cyber security review (0)
- Total (+5)

We did not ignore the fact that there would be some technological cyber security challenges as well as some legal challenges relating to export control, but in the end the overall needs of the organization outweighed the challenges.

This does not mean that these areas of challenge need be ignored. In fact, mitigation activities have been put in place to focus on these specific areas as we proceed into the cloud. This allows us to ensure that we are focusing on the right cyber security efforts and not merely the same efforts that we focused on under the on-premises paradigm.

Procurement

Once this risk assessment is complete and the organization understands whether there is a net benefit for the organization to move into the cloud, it becomes crucial to select the right cloud provider who fits conceptually with the positive risk attributes identified above.

Cloud Provider Relationship

In the past, the relationship between an organization and a provider has been characterized in two main ways. The first model is a product sales and support model. This includes engagement through the initial purchase and the establishment of a support contract to deal with product issues. The product provider is most successful when they can provide a solid product that requires limited support. The more effective that a company is in driving down support incidents, the more they can increase their capacity to be profitable. The support contract becomes an insurance policy against risk for the organization and a residual income for the provider. Providers continually engage the organization in selling additional products as a mechanism to further this type of relationship.

The second relationship model is a service provider relationship. This includes a promised service and engagement through the process until the service is fulfilled. Service providers have a financial interest in ensuring continued service excellence because this is where their residual income arises. Organizations look to get the maximum service for the right price point. Providers look to expand the nature and extent of their service offerings to further this relationship.

Many other types of relationships exist, but these two have been most pervasive across the industry in recent years.

With the cloud, a new and slightly different model is emerging. Although, this relationship has many similarities to a service provider relationship, it has some subtle nuances that are more similar to a product provider relationship. Unlike a project, where costs associated with execution are based on a fixed bid, cost plus fee, or actual costs agreement, a cloud provider costs out their service on a licensing model similar to the product provider. This causes some tension between the organization and the provider because the organization is targeting getting the highest service possible and the provider is looking to establish a residual income stream with as little hands-on activity as possible. Cloud providers cannot and do not ignore customer service, but it is fundamental to understand the dynamics inherent to a provider who is trying to find the ideal balance between cost savings and service excellence. A provider is most effective in focusing on those services that are the greatest value-add and eliminating or automating other non-value add services.

This new relationship is very reliant on both the organization and the provider coming together in a partnership and agreeing up front how this relationship will be managed on both sides. This relationship is not formed after the contract has been signed and the service offering begins, but begins prior to the request for proposal leaving the door.

Statement of Work

With an understanding of the nature of the relationship, it is vital that the organization put together a cohesive statement of work that establishes the basis for what services are critical as part of this relationship. This statement of work needs to clearly delineate which aspects of service are must-haves and which aspects are nice-to-haves.

As INL commenced defining the composition of the cloud e-mail service, we pulled together participants from across the laboratory to participate in a road show of the major cloud providers. The purpose of this road show was not to have the end users choose a provider, but to expose the art of the possible and to assess which features were critical for future success. For many in the laboratory, they had been using the same toolset for 15 years and had settled into outdated paradigms. Establishing a new mindset throughout the laboratory was crucial. Primary organizational contributors were:

- Legal council
- Supply chain management (contracting)
- Records management
- Information technology
- Cyber security

From this and other pre-request for proposal activities, INL was able to collect hundreds of individual requirements. We recognized that establishing the statement of work based on a laundry list of hundreds of requirements would not effectively establish the prioritization of services that was critical in the future relationship. As we looked at our risk assessment, there were some key must-have requirements that rose to the top as go/no-go requirements that had to be met by any provider of the service.

Go/No Go Decision Point

With the nature of our environment, information protection was high on the list of go/no-go requirements. This included ensuring that the provider had the right level of controls in place to protect information. This was verified by the provider's ability to obtain a Federal Information Security Management Act of 2002 moderate level certification that they had been through an independent assessment of controls and had met the minimum qualifications set forth by the Office of Management and Budget [5].

In addition, it was necessary that the provider protect the information both in-transit and at-rest based on the Federal Information Processing Standard. This would ensure that the information was being protected as it traveled across the public network and once it was resident in the provider's data centers [6].

With the challenges associated with both export controlled data and ITAR data, it was important to us to have the cloud provider that could support data centers managed only by U.S. citizens. With the potential sensitivity of this information, either physical export of this information to a foreign country or consumption of this information by a citizen of a foreign country could be considered a deemed export. With U.S. citizen managed hosting facilities, we could ensure that outside of the technical protections guarding our information, we would also have an assurance that those technicians coming in contact with the physical hardware associated with our information did not pose risk to exposure of sensitive information.

Finally, in our environment, we needed to ensure that we had secure access to e-mail through mobile devices. This became an important decision point to ensure that the provider could support the current and future mobility needs of our workforce.

Each provider was required to respond as to how they would meet the go/no-go requirements. Since these requirements could be accomplished in multiple ways, it was important to understand the risk profile associated with the manner in which the provider offered each service.

Technical Requirements

The other requirements gathered during the pre-procurement process were very applicable to selecting the right provider, but were included as ancillary technical requirements. Each provider was asked to respond whether they currently had functionality that met the requirement, whether it was planned on their future product roadmap or whether this was not planned as a future feature set.

This allowed us to get a more complete understanding of the nature of both the product being offered and the nature of the service relationship in production.

Summary

With a risk assessment in place to understand which services are candidates to be moved to the cloud and a carefully defined relationship with the cloud provider, organizations have a strong foundation for effectively managing cyber security in the cloud.

Moving to the cloud is not right for every organization, nor is it viable for every application in their environment, but it can provide significant benefits to the organization when it can be accomplished, such as the business benefits. To be successful in moving to the cloud, organizations have to approach it differently than they have in the past by applying risk-based mitigation instead of merely technological solutions. As INL pursued transforming the manner in which we provide e-mail service to our organization, we learned that through the judicious application of a risk management framework to cyber security we could take advantage of this new service delivery model and still ensure effective information protection.

Disclaimer:

This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

STI Number: INL/JOU-11-22852

ABOUT THE AUTHORS

Troy Hiltbrand is a lead in Information Management (IM) Strategic Planning and Enterprise Architecture at INL. In this capacity, he is involved with coordinating efforts to align IM activities with laboratory strategy and vision and in ensuring that business process, information, technology, and security are brought together in a way that supports the achievement of mission success.

Phone: 208-526-1092
E-mail: troy.hiltbrand@inl.gov

Dan Jones is currently an Information System Security Manager for the Idaho National Laboratory with Battelle Energy Alliance. In this capacity he is responsible for unclassified cyber security, which includes managing the maintenance and operation activities and DOE Program Cyber Security Plan efforts.

Phone: 208-526-6477
E-mail: daniel.jones@inl.gov

REFERENCES

1. Battle of the Aleutian Islands: Recapturing Attu. (2006, June 12). Retrieved March 5, 2012, from HistoryNet.com: <http://www.historynet.com/battle-of-the-aleutian-islands-recapturing-attu.htm>
2. Beyer, R. (2005). The Greatest War Stories Never Told: 100 Tales from Military History to Astonish, Bewilder, and Stupefy. Harper.
3. Subchapter M - International Traffic in Arms Regulation. (1993, July 22). Retrieved April 5, 2012, from U.S. Depart ment of State: <http://pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_120.pdf>
4. Naylor, R., & Smith, C. (2010). Net Generation: Preparing for Change in the Federal Information Technology Workforce. Washington, D.C.: Chief Information Officers Council.
5. Federal Information Security Management Act (FISMA) Implementation Project. (n.d.). Retrieved April 5, 2012, from National Institute of Standards and Technology (NIST): <http://csrc.nist.gov/groups/SMA/fisma/index.html>
6. Federal Information Processing Standards Publications (FIPS PUBS). (n.d.). Retrieved April 5, 2012, from National Institute of Standards and Technology (NIST): <http://www.itl.nist.gov/fipspubs/>