How to Secure the Cloud Based Enterprise Information System

Yanzhen Qu

Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

How to Secure the Cloud based Enterprise Information System

– A Case Study on Security Education as the Critical Foundation for a MS-EIS Program

Yanzhen Qu

Colorado Technical University, 4435 N. Chestnut Street,
Colorado Springs, CO 80907, USA
yqu@coloradotech.edu

Abstract. This paper presents a case study for a new Master of Science in Enterprise Information Systems program created at Colorado Technical University in which security courses occupy over 20% of all classes within the program. Should there be such a high emphasis on security courses? Through reviewing the performance of the first class of students in the Enterprise Information System Capstone course of this program, we can conclude that the investment on the security education is absolutely necessary. These courses have laid down the critical foundation for students to correctly handle today's ever growing real world Enterprise Information Systems' challenges.

Keywords: Enterprise Information System, Security, Security Education, Cloud Computing, Service Oriented Architecture.

1 Introduction

As Enterprise Information System (EIS) becomes an integral part of any modern business, the need to train more qualified IT professionals who can take a business problem and find an EIS solution to address business requirements of the enterprise has become more urgent. To meet such needs, Colorado Technical University (CTU) created a new master program named Master of Science in Enterprise Information Systems in the late of 2008. This program has set up the following core outcomes [1]:

- Plan, implement and use technology within a broad business and real world perspective
- Demonstrate the ability to critically analyze and solve technical issues as they are related to the enterprise
- Demonstrate the ability to design, implement and manage technology solutions to achieve enterprise goals
- Exercise strong interpersonal and team communication skills
- Demonstrate the skills necessary to perform all actions within an ethical framework

The program consists of the following courses:

- Computer Networking
- Security Management
- Database Systems
- Enterprise Systems Architecture
- Enterprise Information Systems
- Information Technology Systems Development
- Project Management Process in Organizations
- Schedule and Cost Control Techniques
- Enterprise Information Systems Capstone
- 2 elective courses from the list course listed below:
  - Software Information Assurance
  - System Security Certification and Accreditation
  - Software Project Management
  - Applied Managerial Decision-Making
  - Project Planning, Execution and Closure Impact on Design & Production

Among all fourteen courses, three courses are related to security. Obviously the security is the heaviest emphasis in this new program. This results from the combination of the market trend research and the recommendation from the CTU's industrial advisory board. Because security issues are associated with every component of the EIS, every application, and every business process, it is no longer enough to just provide students with some basic concepts and common practice knowledge in security management. It is very important to make students understand the root cause of all the security issues, the essence, principles and methods of security management, and the impact of security to every decision made by an EIS designer or developer. In fact, as a "National Center of Academic Excellence in Information Systems Security Education" designated by the US National Security Agency and the Department of Homeland Security, CTU has always placed a high emphasis on security education in its Computer Science and Information Technology degree programs in all levels from Associate, Bachelor, and Master to Doctor.

In January 2010, the first cohort of students enrolled in this new program was about to take their EIS Capstone course. The students were to be tested on how well they could solve real world problems by applying the knowledge and skills they had acquired from the new program. At the same time this new program was also to be tested on how effective its courses were. Having taught several courses with this cohort, recommended by both the school and the students, I was selected as the instructor for this first EIS Capstone course.

In the following sections I will present a case study of the EIS Capstone course so that we will have some evidence to answer the question: "Is the emphasis on security in this new program a right decision?"

Interestingly enough, the answer to that question is closely related to the answer to another more technical question: "How to secure the Cloud based Enterprise Information System".

The rest of this paper will help relate those two questions.

2 What are the Real Requirements?

This first EIS Capstone course was sponsored by the global Information Technology (IT) department of a multi-national enterprise. For convenience, in the rest of this paper, we will call this enterprise "the Company." The EIS Capstone course was scheduled for 11 weeks, and this cohort had total of 12 students. During the first week of the class, we went through the requirements of the EIS Capstone class and also reviewed various key concepts of Service Oriented Architecture and Cloud Computing [2], [3]. During the second week of the class, our sponsor met with all the students, and issued a written task specification as shown below (minor wording modifications have been made correspondingly) [4]:

"The Information Technology (IT) department serves the global technology infrastructure needs of the Company through the stewardship of scarce financial, human, software and machine resources. The Company has set as its goal to double its service to the targeted customers by the year 2015 and double again by the year 2020. In anticipation of supporting this goal, IT will complete installation of a global technology infrastructure upgrade by June 2010.

In addition to internal Company's resources, IT envisions leveraging an agile global pool of technical resources to assist in the construction and deployment of our technical service offerings. Service offering outcomes may include technologies that link suppliers to customers, address specific community needs, and enable real time responses from venders or suppliers to global needs.

Task Description:

In consideration of Vision 2020, global technology infrastructure upgrade, the current IT architectural and investments, will establish an executive level plan to establish a global developer network that:

- *Articulates a global vision, outcomes and benefits*
- *Describes the objectives and scope of the plan*
- *Frames and describes the required technical infrastructure, standards and processes required*
- *Outlines the sequence of proposed activities and dependencies*
- *Documents risks and mitigation strategies*
- *Provide a rough order of magnitude costs to implement*
- *List assumptions that bound the scope and delivery of the project "*

After reading through this task specification, all students asked the same question: "What are the real requirements?" This was because they were lacking the working knowledge regarding the Company's As-Is IT systems, the daily real challenges and restrictions that the Company's IT department faced, and the root cause of these problems. Therefore, the students decided that they first needed to start the system life cycle development process to make more in-depth investigations, and to exercise more due diligence to find out the real requirements.

Through a sequence of email communications and several face to face meetings, much more information was collected, as summarized in the following:

- The Company was helping more than 1 million customers in 25 countries with an ever growing need. It was essential that the Company expands its system-wide IT communication capability to automatically translate, store, secure, update, and rapidly retrieve large amounts of data.
- The protection of the Company's business databases which include the financial information of their partners, vendors, suppliers, and customers, was a crucial requirement.
- The Company's existing IT systems were developed by multiple vendors and introduced at different times for different purposes. The Company's As-Is IT systems were really the Silos systems as described in [5]. All the IT functions had been independently structured to meet local application demands with only a secondary consideration on how to connect a global community. The IT functions also did not readily share information outside of their respective infrastructures.
- With the limited IT budget that the Company could offer, developing any new integrated EIS would require a very innovative and non-conventional solution. And the Company was willing to look into any new technical solutions that could save costs while still achieving its' final goals.

It was very clear that the real requirements could be concluded in one statement:

"***The Company needs to develop a Service Integration Architecture Framework to enable existing and new functionalities and resources continuously integrated in a fast, secure and cost efficient manner."***

This statement was quickly reviewed and endorsed by the sponsor. It then not only provided the project direction for students, but also became the only criteria to assess the final result of the students' work created through the project.

3 A Solution Meeting the Requirements: Service Integration Architecture Framework based on Cloud Computing [6]

After fully understanding what the real problems of the As-Is IT systems were and what real needs the Company had, the students quickly focused their effort onto creating a new Service Integration Architecture Framework (SIAF). The SIAF would help the Company not only to move from the Silos systems to an integrated Service Oriented Architecture (SOA) based system, but also to take advantage of Cloud Computing Services wherever appropriate.

As shown in Fig. 1, the proposed SIAF addressed the pre-requisite considerations and risks associated with external Cloud Computing Services and/or platforms to include newly evolving issues, constraints, efforts, technical advances, and the latest industry standards pertains to the Company's global operations.

In the proposed SIAF, the discussions were focused on the following five aspects:

(1) Pros and Cons of Various types of Cloud Computing Services
(2) Security in the Context of Cloud Computing:

- Identity and Access Management
- Data Security

(3) Communication in the Context of SOA and Cloud Computing:

- External Enterprise Service Bus (EESB)
- Internal Enterprise Service Bus (IESB)

(4) Application Programming Interface
(5) Business Process Manager

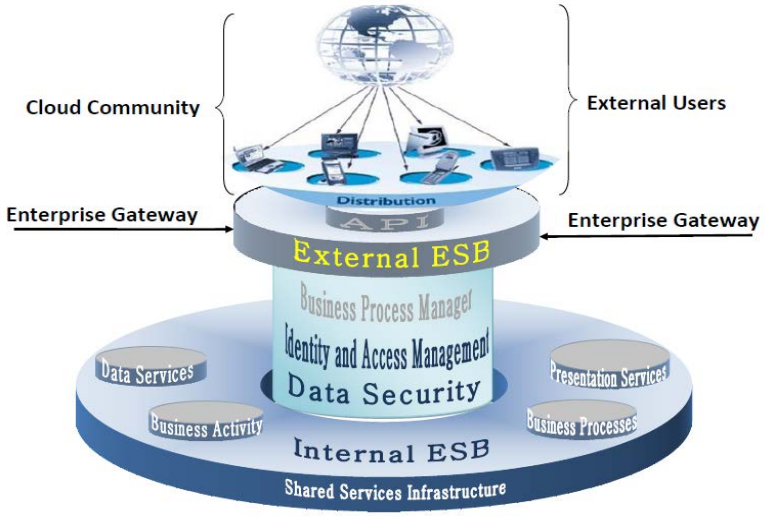

Fig. 1. Service Integration Architecture Framework

Below is the simplified version of students' proposal.

3.1 Pros and Cons of Cloud Computing Services

The students provided a through analysis on the Pros and Cons of various types of Cloud Computing Services regarding the needs of the Company, as summarized in the Table 1.

The students concluded that although public Cloud Computing Services could provide cost savings on both IT Application and Data Management, the cost to maintain the required security and privacy as well as data accessibility would reduce that benefit. The entire IT Operation cost would only be reduced to a certain level depending on what type of Clouding Computing Service was really used.

3.2 Security in the Context of Cloud Computing

Security functionality is the central part of in this SIAF. It is managed through two subsystems: Identity and Access Management (IAM) subsystem and the Data Security subsystem.

Table 1. Comparisons of Various Types of Cloud Computing Services

Type of Cloud Computing Service	Private Cloud (On Premise)	Public Cloud–IaaS (Infrastructure as a Service)	PublicCloud-PaaS (Platform as a Service)	PublicCloud–SaaS (Software as a Service)
Control Computing Resources	Organization Control	Shared Control	Vendor Control	Vendor Control
Data Security and Privacy Risk	Low	Medium	High	High
Data Management Cost	High	Medium	Low	Low
Existence and Standards for Cloud Identity and Access Management (IAM) Tools	Matured (ISO/IEC27002)	Reviewed (ISO/IEC27002 (2005))	Proposed (Cloud Security Alliance established in 2008)	Proposed (Cloud Security Alliance established in 2008)
Requirements for Federation IAM Tools	Lowest	Low	Medium	High
IT Application Development Cost	Highest	High	Medium	Low
Security and Privacy Management Cost	Low	Medium	High	Highest
IT Operation Scalability	Low	Medium	High	High
Overall IT Operation Cost	High	Medium(high end)	Medium	Medium (low end)

IAM Subsystem

The IAM subsystem includes the following components:

- Access control based on business requirements
- User Access Management
- User Responsibility validation and enforcement
- Network access control
- Operating system access control
- Application access control
- Information access control
- Mobile computing and teleworking access control

The IAM's purpose in the context of the Cloud Computing is to extend and blur the lines of boundary and trust. It must achieve the following security functionalities:

- Timely and secure managing of on-boarding and off-boarding users in the cloud.
- Authenticating users in trustworthy and manageable manner and addressing credential management, delegation, and managing trust across multiple types of Cloud Computing Services.
- Federation to enable organizations to use selected Identity provider (IdP) to exchange identity attributes across allied organizations.
- Authorization and user profile management to establish and manage profiles and policies to control access in auditable manner.

Data Security Subsystem

In addition to the conventional data security functions that are usually associated with the specific data management systems (such as databases, or data warehouses) in the context of Cloud Computing, the data security subsystem must also support the following functionalities:

- Arranging different data stores and accessing measures based on the security level, availability and integrity requirement of the data.
- Effectively supporting the responsibility in terms of Physical Administrative Access, Logical Administrative Access, Object Sharing and Maintenance of the data which are well defined in the Service Level Agreement (SLA).
- Being able to test and verify the capabilities of the Secured and Virtual Storage, Disaster Recovery or Continuity of Operation declared by the cloud service providers.
- Being flexible enough to smoothly switch among the various mode of an IT application's lifecycle such as "application development mode", "application testing mode", "application operation mode", "application maintenance mode", and "application retiring mode", etc.

3.3 Communication, API and Business Process Manager

The Internal ESB is responsible for managing and interacting with the Company's current information at its Core IT Infrastructure. For example, the Internal ESB can manage and increase capability to communicate with Field Offices and Partners.

The External ESB is responsible for managing Cloud Computing Services in the future and the connection to external APIs to utilize the Cloud Computing based applications.

As a component allowing the external users or applications to integrate with the Company's applications, the Application Programming Interface (API) is a critical "gateway" between the external world and the internal Core IT Infrastructure.

The Business Process Manager subsystem is responsible for invoking Business Processes defining the work flows for both internal and external communication.

3.4 Final Recommendations

Finally, the students recommended the Company to carefully examine the following actions to develop their next generation IT system infrastructure.

- Until the Cloud security management matures, consider migration of only non-sensitive data and low risk applications as a logical first step.
- Develop more mature Identity and Access Management capabilities within the enterprise while the Cloud Computing Service community coalesces.
- Utilize ESBs to route and translate messaging for both internal and external users, which sets the stage for the Company to adapt to Cloud Computing.

4 Conclusion

After the SIAF was presented to the executives and IT management of the Company, it received high praise from the audience. It was commonly acknowledged that the most impressive achievement by the students was that they had correctly considered security at every level of the system. They also successfully balanced the benefits and risks involved in the Cloud Computing. The most attractive feature of their proposal was that it enabled the Company to gradually replace future applications development with Cloud Computing Services, while, smoothly and securely integrating these results with the Company's own Core IT Infrastructure. The students work had fully met the requirement. And the objectives of the program were also met completely.

During the final discussion on the project, most of the students had credited their success back to the security courses taught in the program, which had prepared them well for dealing with the security related issues in the project.

Therefore when the students correctly answered the question: "How to secure the Cloud based Enterprise Information System", and succeeded in their EIS Capstone project; our question: "Is the emphasis on security courses right?" had also been clearly answered. Indeed, the security education in the MS in EIS program played a critical role in our students' success.

References

1. Colorado Technical University: 2009 Course Catalog. (2009)
2. Linthicum, D. S.: Cloud Computing and SOA Convergence in Your Enterprise. Addison-Wesley(2010)
3. Mather, T., Kumaraswamy, S. and Latif, S.: Cloud Security and Privacy Enterprise. O'Reilly(2009)
4. Qu, Y.: Internal Communication Note. (2010)
5. Goyal, B. and Lawande, S.: Enterprise Grid Computing with Oracle. Oracle Press USA (2006)
6. Windom, S., Hasse, M., Chaney, L., Salinas, M. and Rademacher, T.: Service Integration Architecture Framework. Colorado Technical University Technical Report(2010)

Acknowledgement
The author sincerely thanks all the students who participated in the EIS Capstone class described in this paper. Much of the technical content and the conclusions made in this paper about the Service Integration Architecture Framework project are directly based on their excellent work.