Transforming Security Through a Public Cloud Migration

Critical Challenge Project, Executive Master in Cybersecurity

February 2, 2018

Katie Jenkins, EMCS ‘18

Dr. Ravi Pendse, Advisor,

Vice President and Chief Information Officer, Brown University

This Critical Challenge Project (CCP) deliverable is an extract from the full report. The guidance contained herein may be shared with the broader Brown community, unlike the full report.

Executive Summary (Abbreviated)

This CCP supports the premise that a cybersecurity program can be improved through a public cloud migration with the right amount of planning and emphasis on the security imperatives.

It was with this perspective and work in preparing a one-hundred-year-old insurance company for one of the most significant technology and business transformations ever experienced, that the following three deliverables were created and can be used by other organizations considering a migration to public cloud:

1. **Appendix A: Model Security Organization**: What talent and team structure are needed to plan for and implement a secure migration to the public cloud
2. **Appendix B: Training Plan**: What skills are needed to transform the talent and culture of an IT team moving to the public cloud
3. **Appendix C: Reference Guide for Enterprises**: What questions and considerations must enterprises concern themselves with when planning for a secure migration

This guidance for enterprises spans the people, cultural, and technology dimensions of a secure public cloud migration and reflects the lessons from EMCS coursework; research; cloud training; discussions with cohort members, vendors, and cloud service providers; and real experiences in organizational planning and design.

Appendix A: Model Security Organization

These tables represent a functional structure of a team supporting a secure cloud migration. The approximate size of the organization this structure is intended to support is 10,000 users and 1000+ applications. Team size can be scaled accordingly.

Cloud Enablement Director		
Team Name	***Team Composition***	***Team Description***
Cloud & Security Innovation & Enablement	• Manager • Sr. Product Owner • Cloud Engineers (3) • Security Engineer • Cloud Architects (2)	Quickly and securely enable services and capabilities needed for application and platform teams within the cloud
Cloud Services	• Product Owner • Scrum Master • Cloud Engineers (5) • Data Analysts (2) • Security Engineer • Cloud Architect • QA • Developers (2)	Deliver cloud services through pipeline driven automation and orchestration for self-service developer enablement
Application Enablement (the number of Agile teams of this composition can scale up depending on the number of development functions being supported)	• Manager • Product Owner • Scrum Master • Associate Product Owner • Cloud Engineers (8) • Developers (2) • Security Analyst • Security Architect	Provide customer and/or platform centric aligned cross functional team to further enable re-platforming, re-factoring, and re-architecting their current applications while leveraging new platforms and services within the cloud
Success Criteria: Leading on new technology adoption, new application development, and modernization of existing applications by leveraging advanced cloud computing capabilities will increase security and speed to market while reducing long-term expenses and further empowering application teams through self-service models.		

Security Enablement Director		
Team Name	***Team Composition***	***Team Description***
Compliance & Security Operations	• Manager • Associate Product Owner • Compliance Analysts (4) • Security Analyst (6)	Maintain compliance of financially significant systems; Optimize and deliver security operations
Security Solutions Delivery	• Manager • Scrum Master • Security Analysts (9)	Deliver CISO Office and Business Unit Security prioritized efforts
Cloud Security & Engineering	• Manager • Product Owner • Scrum Master • Risk Analysts (3)	Transform security controls to automated and self-enforcing cloud controls, assess cloud risk

	• Security Engineers (3) • Security Analyst • Developer (2) • Data Analyst (2) • Security Architect	
Success Criteria: Protecting technology assets through the development and adoption of automated, self-enforcing security controls while sustaining compliance for financially significant systems. This implementation of automated security controls will enable development speed, securely.		

Appendix B: Training Plan

This training plan assumes a mature IT workforce with deep understanding of application, network, and security architectures but lacks knowledge and experience with public cloud principles and security control implementation in public cloud environments.

Through partnership with the cloud service provider, established training vendors, and in-house expertise, the objective is to offer educational curriculums to train team members on the new technology and new ways of working (i.e. Agile).

It is expected that trained team members positioned to work in an agile manner to design and implement a security architecture in a public cloud environment, minimize the need to replace workforce with external experienced hires.

Skill Needed	Desired Outcome	Course Name	Management	Security Analysts	Security Engineers	Security Architects	Compliance Analysts	Risk Analysts	Data Analysts	Security Operations	Developers	Cloud Engineers	Cloud Architects
Agile	*Understand the fundamentals of SAFe, understand agile roles, prepare for formal transformation and training*	Agile Self-Guided Training (standard curriculum)	★	★	★	★	★	★	★	★	★	★	★
		Agile Leadership	★										
Introduction to Cloud Computing	*Understand the basics of cloud computing; SaaS, PaaS, and IaaS models; intro to storage, compute, and other cloud services.*	AWS Fundamentals	★	★	★	★	★	★	★	★	★	★	★
Advanced Courses in Cloud Computing	*Develop advanced skills in IT professionals with cloud experience to accelerate adoption of cloud services and establishing security patterns.*	Architecting on AWS				★						★	★
		Advanced Architecting on AWS				★						★	★
		DevOps Engineering on AWS									★	★	
		DevSecOps Workshop		★	★					★	★		
		Expanding AWS Adoption										★	★
Specialty	*Develop skills to specialty functions, like audit and compliance, operations and development (both within the Cloud & Security Enablement organization and partner teams).*	Cloud Native Workshop for Developers									★		
		Security Operations on AWS (Intermediate level)		★			★			★			

Figure 5. Sample Training Curriculum

While the above training courses are largely specific to, or offered by AWS, training should be tailored to the needs specific to which cloud service provider selected. For example, training offered by Microsoft can be found here: https://azure.microsoft.com/en-us/training/?v=17.50

Appendix C: Preparation Guide for Enterprises

Introduction

As enterprises seek to leverage the vast opportunities for speed, innovation, and agility offered in public cloud computing infrastructures, security must remain a 'top of mind' consideration. Getting to the cloud quickly without thoughtful planning for security can be disastrous for an enterprise. Meanwhile, never gaining the benefit of the cloud for fear of potential security risks, can hinder the growth and innovation an enterprise needs to remain a competitive and thriving company. This guide has been prepared by an IT and Security leader in a one-hundred-year-old financial services company as a reference to those who share similar aspirations in maintaining or elevating an organization's security posture through a public cloud migration.

Step-by-Step Guidance

1. **Take stock.** Asset management is important to virtually all aspects of IT, and preparation for a public cloud migration is no different. Consider:
    - **a.** What are your big "monolithic" applications?
    - **b.** What are your modernized apps that adhere in full (or to a large degree) to the 12 Factor App methodology[3]?
    - **c.** What is your inventory of OS, database, and middleware technologies?
    - **d.** Do you presently use a CI/CD pipeline for code deployments?
    - **e.** Have you appropriately classified your IT assets into those which are financially significant, regulated, and/or externally facing?
    - **f.** What are your data residency needs? Do you have data of non-US based individuals subject to specific regulatory requirements like GDPR?
    - **g.** Is avoiding vendor lock-in a primary consideration for your IT leadership?
    - **h.** Are you culturally ready for a public cloud migration? The opposing ends of this spectrum might be:
        - **i.** Your leadership is ready to go; you are scrambling to hold them back long enough to think through your security strategy
        - **ii.** There is great reluctance in moving to the public cloud; you are in a position to positively influence this undertaking
2. **Talent Assessment.** Culture and people are critically important to the cloud journey. The technology is the far easier part. Consider:
    - **a.** Do you have talent skilled in public cloud computing?
    - **b.** Does your organization have the training resources to commit to educating the existing workforce?
    - **c.** A sample training plan is included for reference in Appendix B.
3. **Identify Your Team**. There are many players necessary to the success of public cloud migration. A sample organization structure has been included for reference in Appendix A. Apart from the IT functions necessary for the journey, such as network, systems, and security architects, developers and engineers, compliance and controls specialists, and database experts, there is a large group of partner teams who also are part of the extended team. These parties include:

   a. *Internal Audit* who needs to prepare for controls evaluation in public cloud environments
   b. *Legal and contracts* folks who need to evaluate if any existing customer contracts expressly forbid data processing in off-premise environments
   c. *Customer Account Managers* who need to socialize the change with enterprise customers and facilitate contract addendums as needed to allow for this change in computing environments
   d. *Procurement* to manage the lengthy negotiations with the cloud service providers and existing vendors for whom current license agreements may require a change to move from an on-premises to public cloud license model.
   e. *Finance* to evaluate and model the costs in moving the cloud, including considerations of bring your own license (BYOL) or having the cloud provider provide the needed licenses.
4. **Identify a Starting Point.** At some point it becomes necessary to take a bold step to begin experimentation in the public cloud. Sandbox environments, test datasets, and well-defined stakeholders and objectives can have significant benefit in realizing what is possible.
   a. Involve your security team in all pilots. They can help evaluate the control needs and influence design and architecture early on, as pilots can quickly evolve to a production state.
   b. Keep the pros and cons of cloud vendor services versus approaches that minimize vendor lock-in at the forefront of initial decisions. Getting too tied to native services offered by your cloud provider could be difficult to untangle later if your IT leadership prefers avoidance of vendor lock-in.
5. **Document a Control Framework.** Consider the existing control framework(s) that your existing security program is based on (or aspires to). This could be the NIST Cybersecurity Framework[4]. There are existing cloud-specific frameworks as well, such as ISO 27018[5] which offers controls for the protection of Personally Identifiable Information in public cloud computing environment, aligned to commonly accepted privacy principles. Additionally, the Cloud Security Alliance has a Cloud Controls Matrix[6] for reference. With these frameworks already developed, it is unlikely you need to work from scratch in developing your own, but specific circumstances might warrant that. With a controls framework identified, the next step is to perform an analysis of which controls are your "non-negotiables" versus "nice to haves." Next consider whether there is portability of your on-premise controls, or do the controls need to be re-architected for the public cloud environment.

   Here is an excerpt from the roughly 380 controls sourced from the Unified Compliance Framework®[7] a draft mapping to applicable regulatory requirements, noting which controls the enterprise deemed necessary in the public cloud environment.

Ref #	CTRL Name	Category	EU GDPR	CIS 20 Critical Sec Ctrls	NIST Framework	New York State Dept of Financial Svcs	Cloud Controls
102	Implement two-factor authentication techniques.	Access and Authentication		Control 11		500.12 (a)	X
103	Establish and maintain an encryption management and cryptographic controls policy.	Encryption				500.12 (b)	X
104	Encrypt restricted data using the most secure method possible.	Encryption		Control 16			X
105	Establish and maintain cryptographic key management procedures.	Encryption					X
106	Authorize transactions of data transmitted over public networks or shared data networks.	Network Management					X

Figure 6. Excerpt from control framework mapping.

6. **Establish and Communicate Cloud and Security Principles Early.** To avoid surprises with your development teams, set security expectations early. Examples of cloud and security principles might be:
    a. All new development should be cloud ready.
    b. Data in public cloud environments are encrypted at rest and in transit. No exceptions.
    c. All code is released through a pipeline.
    d. Logging and monitoring is required on all cloud workloads.
    e. Use enterprise credentials for user identities (e.g. cloud provider federation with corporate IdP).
    f. Forced rebuild of application stack at defined intervals.
7. **Tackle Big Needs Early.** Some things are easier to change over time than others. Two examples of architectural decisions that need careful thought up front are:
    a. Account Design – in AWS, defining accounts and availability zones are critical to establish initial structures for your cloud presence, minimize the blast radius, establish a basis for access control, address data residency needs, and potentially support BCP and DR needs.
    b. Identity and Access Management – The ability to ensure authorized access to assets by users or resources, known as Identity and Access Management (IAM) is one of the more complicated facets of preparing for security in the cloud. The significance of sound architectural decisions, such as designating the authoritative source for identities, is amplified by the risk surrounding the complex web of on-premise, cloud based, or multi-cloud based users and assets. User and resource identity, or how to create, store, and manage these identities, is a first consideration. Access models are another early consideration. Consider:
        i. Is single sign on (SSO) a requirement?
        ii. Will you need two-factor authentication?
        iii. What are your needs for federation with third parties?
        iv. What are your logging and oversight needs?

v. Is a zero trust model an upfront design consideration?

Regulatory and compliance needs are strong influencers in this space. As this topic could warrant its own CCP, the guidance from the Cloud Security Alliance in its Identity, Entitlement, and Access Management Guidance[8] is a highly valuable reference. Opportunities to take advantage of stronger authentication schemes and modern IAM protocols present rich opportunities to introduce improvements over existing security practices.

8. **Communicate is Key.** Let your team know of progress and challenges. Sponsor regular demos of work or 'lunch and learn' sessions. It will motivate those involved in cloud efforts and bring awareness to those teams not yet part of the migration.
9. **Get connected.** Many groups are focused on security in the cloud such as https://cloudsecurityalliance.org/. Learning from others and contributing to others' understanding of security in the cloud will help advance progress in this growing field.