A Systems Perspective on Cybersecurity in the Cloud – Frameworks, Metrics and Migration Strategy

by

Ravi Raina

Bachelor of Engineering (Hons) Electrical and Electronics Engineering (1998)
Birla Institute of Technology and Science, Pilani

Master of Science Computer Engineering (2002)
North Carolina State University

Master of Business Administration (2016)
Cornell University

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

September 2016

Signature of Author Signature redacted

Ravi Raina
System Design and Management Program
August 12, 2016

Certified by Signature redacted

Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management
And Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Accepted by Signature redacted

Warren Seering
Weber-Shaughness Professor of Mechanical Engineering

[Page intentionally left blank]

A Systems Perspective on Cybersecurity in the Cloud – Frameworks, Metrics and Migration Strategy

By
Ravi Raina

Submitted to the System Design and Management Program on Aug 12, 2016 in Partial fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management.

Abstract

Cloud computing represents the next generation of disruptive technologies in computing. However, there are several barriers to massive adoption of cloud and among them security remains one of the principal concerns. Traditional failure analysis and prevention frameworks fall exceedingly short to address cybersecurity as is evident by every increasing cybersecurity breaches. New frameworks for cybersecurity are required which take a holistic view of the problem and a systems perspective. Migrating to cloud also represents a key decision point for CEO/CTO's today, especially from security perspective.

The objective of this thesis is to illustrate the effectiveness of taking a Systems Approach to cybersecurity and provide a framework for migration to cloud with specific emphasis on critical cybersecurity issues pertaining to various cloud deployment models and delivery services.

The thesis is divided into three phases. Firstly, it will aim to explore the major security threats and critical areas of focus for security in cloud. It will explore the major security frameworks, metrics and controls, especially the major ones from NIST, CIS and CSA. SLA's for different cloud service models will then be presented. A high level cloud migration framework strategy and framework, with special emphasis on cybersecurity will also be discussed. In the second phase, System-Theoretic Accident Model and Processes (STAMP) which is based on Systems Theory will be applied to Target security breach and key recommendations as well as new insights will be presented. The analysis will highlight the need for holistic approach and Systems Thinking to cybersecurity and new insights that are not produced by traditional methods will be presented. Finally, in the third phase, the cloud migration framework discussed in phase one will be applied to Target. A case will be made that in certain scenarios, moving the less critical applications to cloud and utilizing the security benefits of cloud can actually reduce the threat vectors and security exposures and bring IT systems from a higher risk state to lower risk state.

The thesis integrates cybersecurity methods and frameworks as well as security metrics with the cloud migration strategy. Additionally, it also presents STAMP/CAST failure model for cybersecurity breaches and highlights the need for integrated view of safety and security and Systems Thinking in cybersecurity both in traditional systems and cloud.

Thesis Supervisor: Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management
And Professor of Engineering Systems, MIT School of Engineering

[Page Intentionally left blank]

Acknowledgements

I would first like to thank the Almighty and my Spiritual Guru for his guidance, inspiration and unending love and fulfilling my dream to pursue higher studies at MIT and letting me experience this incredible intellectual journey. These past two has been a truly transformative and enriching experience for me and have expanded my horizon and worldview.

I am extremely grateful to several people who have played instrumental role in thesis and my journey at MIT. First and foremost, I would like to thank my advisor, Prof. Stuart Madnick, for his constant support and mentorship. He has been a source of inspiration and I am grateful for his insight, instruction and guidance. He dispelled obscurity, darkness and ignorance and led me to clarity, light and learning. He patiently reviewed several iterations of final work, leading to its culmination. It has been an honor and privilege to work with him and I will forever be in gratitude. Thanks to Allen Moulton and Raphael Yahalom for their valuable insights and encouragement during my thesis presentation.

A special thanks to SDM Program Director, Pat Hale and SDM staff for building and nurturing an excellent program like SDM. Thank You Pat, for being a pillar of support, encouragement and guidance and providing a safe harbor during rough seas. I would also like to thank Bill Foley for his support throughout the two years. Thanks to all the wonderful people I have met at the program and friends I have made at both MIT and Cornell. Thanks for your loyalty and selflessness. I will always cherish our friendships. It has been a privilege to be part of SDM at MIT and be in the company of incredibly gifted people. SDM has let me experience the true meaning of "Mens et Manus" and truly transformed the way I look at the world and global challenges.

I would also like to thank my family without whose support and sacrifice, I wouldn't be here today. My mother and father provided source of inspiration, believed in me and always encouraged me to pursue my dreams and teaching me the value of humility, perseverance and industry. Thank your sister for being there for me always. It's only because of you all, that we survived storms together including terrorism and came out stronger. I would also like to thank my wife Pragati for her love and encouragement and supporting me throughout this journey, taking over responsibility so I could focus on studies at both MIT and Cornell. Would also like to thank my children, Arin and Adhya for their refreshing innocence, quiet patience and unwavering love. My gratitude to Pragati's parents also for their love, support and sacrifice through this entire time. Special thanks to my Golden Retriever, Juno, for her love, loyalty and being the greatest stress buster.

I dedicate this thesis to my mother, who has been the foundational bedrock of my life and guiding light of our family. Whatever I am today is because of your unconditional love, boundless inspiration and belief in me. Mom, words can never express the deepest gratitude I have for you.

"Om. Lead me from the unreal to the Real, Lead me from the darkness to the Light,
Lead me from the temporary to the Eternal, Om. Peace, Peace, Peace."
— Brihadaranyaka Upanishad 1.3.28

[Page Intentionally left blank]

Table of Contents

List of Figures

List of Tables

Glossary

Attack Vector - A path or means by which a hacker can gain access to a computer or network in order to cause a damaging outcome.

Causal Loop Diagram: a simple map of a system with all its constituent components and their interactions.

Cybercrime: an offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks.

Cybersecurity: the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Denial-of-service (DoS): a type of cyberattack that intends to bring an online service down by overwhelming the system limit with massive traffic, which can come from many locations and sources.

Distributed Denial-of-Service (DDoS): a type of DoS where multiple systems infected with a Trojan are used to conduct DoS attacks on a single system.

LR: Liberty Reserve was a centralized digital currency service that allowed users to register and transfer money to other users with only a name, e-mail address, and birth date. No efforts were made by the site to verify identities of its users, making it an attractive payment processor to scam artists.

Malware: malicious software as the software's creation intent is malicious.

System: an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements.

System Thinking: centered in context, interfaces and emergent behaviors – the interstitial elements around and within the system; the "whole" rather than the decomposed element. [Pat SDM]

Abbreviations

Abbreviation	Description
AWS	Amazon Web Services
API	Application Programming Interface
APT	Advanced Persistent Threats
CAST	Causal Analysis based on STAMP
CIO	Chief Information Officer
CIS	Center for Internet Security
CPS	Cyber Physical Systems
CSA	Cloud Security Alliance
CSO	Chief Security Officer
CSP	Cloud Service Provider
CTO	Chief Technology Officer
CTU	Counter Threat Unit
DOJ	Department of Justice
ENISA	European Union Agency for Network and Information Security
FTA	Fault Tree Analysis
ISO	International Standards Organization
MSS	Managed Security Services
NIST	National Institute of Standards and Technology
OS	Operating System
PCI-DSS	Payment Card Industry - Data Security Standard
PoS	Point of Sale
QFD	Quality Function Deployment
ROI	Return on Investment
RFP	Request for Proposal
SCCM	System Center Configuration Manager
SEC	U.S. Securities and Exchange Commission
STAMP	System-Theoretic Accident Model and Processes
US-CERT	United States Computer Emergency Readiness Team

1: Introduction to Cloud Computing

"We are all born with a divine fire in us. Our efforts should be to give wings to this fire and fill the world with the glow of its goodness. All Birds find shelter during a rain. But Eagle avoids rain by flying above the Clouds." — A.P.J. Abdul Kalam, Wings of Fire

1.1 Cloud as a Computing Paradigm

Cloud computing is an emerging paradigm considered to represent the next evolution of disruptive technologies in computing. While there are multiple definitions of cloud computing, sometimes simply referred to as "cloud", it essentially provides access to configurable computing resources (e.g. storage, networks, servers, applications and services) and on-demand over the internet or other networks, as a measurable and metered service (e.g. pay-per-use basis). According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [NIST 2011].

Cloud relies on sharing of resources to achieve economies of scale, much like a public utility such as an electric grid. It essentially makes computing, a public utility. As such, it offers all the advantages of a public utility system, in terms of economy of scale, flexibility, convenience but it raises major issues, especially loss of control of sensitive information and loss of security [Wikipedia – Cloud].

Cloud has been brought about by the convergence of several existing and new technologies, namely high capacity networks, low cost computation and storage, as well as adoption of virtualization, service oriented architecture and autonomic computing. According to IDC, Gartner, Microsoft and other research consultancies, Cloud computing and services are one of the fastest growing segments in IT and are projected to maintain their rapid growth well into the next decade.

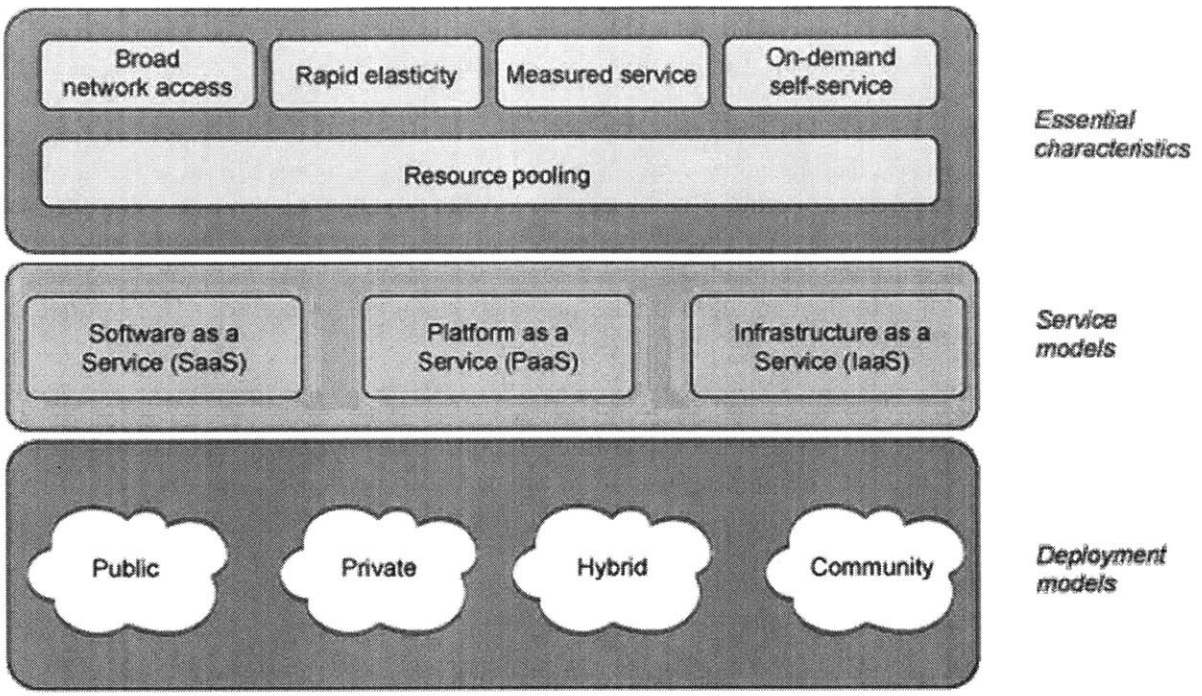


Figure 1.1: Visual Model of NIST Working Definition of Cloud Computing [NIST -ITL, Cloudbolt 2016]

Figure 1.1 provides a visual model of the definition of cloud by NIST. This definition lists five essential characteristics of cloud computing: On-Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity or Expansion, and Measured Service. It also lists three "Service Models" (software as a service, platform as a service and infrastructure as a service), and four "Deployment Models" (public, private, hybrid and community) that together categorize ways to deliver cloud services. These definitions will be discussed further in the coming chapters.

1.2 Key Characteristics of Cloud

Some of the key characteristics of cloud, which makes it particularly attractive to both individual users and enterprises include [CSA 2009, AWS EC2]:

On-Demand Self-Service
A customer can request computing resources and services (e.g. storage, databases, applications) on demand automatically without requiring human interaction with the cloud service provider. The cloud provider can meet the demands of the customer much quicker than a typical internal IT organization, deploying the resources from days to hours or even instantly.

Broad Network Access

The cloud capabilities and resources are available over the network and can be accessed through standard thin or thick client platforms (e.g. mobile phones, tablets, PC's) as well as other traditional platforms or cloud based services.

Resource Pooling
The cloud service provider's computing resources are pooled together to serve a spectrum of customers using a multi-tenant model. The different physical and virtual resources are dynamically allocated according to consumer demand. There is a sense of location independence and customer has no control over the physical location of the provided resources or services (e.g. storage, compute capacity, software).

Rapid Elasticity
The customer can rapidly provision cloud capabilities, in most cases automatically, according to its dynamic needs. This means computing resources can be scaled up or scaled down elastically, commensurate with demand. This reduces the burden of planning capacity in advance in a traditional data center (which can result in either opportunity cost or lost customers) and actual demand closely follows acquired capacity.

Measured Service
Cloud provides a measured service, much like public utility such as water and electricity. Resources are automatically controlled and monitored at some level of abstraction which is appropriate to the type of service. This monitoring of resources provides transparency to both the cloud provider and consumer.

As a result of the above characteristics, cloud provides several key benefits which makes it attractive to users and enterprises alike. Some of the key benefits of cloud services include [AWS EC2]:

Speed and Agility
In cloud computing, developers have access to new software, computing resources and applications with only a click away, resulting in more agility and reduced development times. This can result in dramatic increase in agility as the development resources required to build products and services are just a click away.

Accessibility and Flexibility
Applications and services are not locked onto particular locations or devices and can be accessed anytime, anywhere as long as one has network connectivity. Most cloud providers also provide mobile apps, so the users can truly have global access to their data and applications. This feature can also businesses to allow flexibility in work schedules and they can telecommute.

Reliability
Cloud providers generally use multiple redundant sites which increases system reliability. This is very important for business applications and during unforeseen events (e.g. natural disasters). Most big Cloud Service Providers (CSP) are extremely reliable in providing their services with very high uptimes.
Going Global

Companies can go global in minutes, by having access to cloud resources. This is especially advantageous to startups and small companies, who don't have the resources to invest in data centers and want to be the first to market their ideas and products.

Less Upfront Capital Expenditure
In house data centers require huge capital expenditures. Companies have to make significant investment upfront in hardware, facilities etc., before they can get the value and benefits. In cloud, expenses become variable cost and one only pays for how much one consumes.

Benefits of Massive Economies of Scale
Big cloud providers like AWS and Microsoft Azure have built enormous cloud infrastructure providing massive economies of scale. They cater to a very large pool of users and hence many expenses and fixed costs get distributed over a very large user base. Cloud providers also have energy efficient data centers as they have the resources and scale. These benefits are transferred to the users and translate to lower subscription and pay as you go prices.

Do Away with Guessing Capacity
For data centers, companies have to estimate future demand which is seldom inaccurate. So resources can be underutilized leading to capital waste or more capacity could be required, which takes time and could result in business opportunities lost. With cloud, one eliminates the need for guessing infrastructure capacity needs and only pay for resources (e.g. infrastructure capacity, applications) as and when it is required and can scale up or scale down as necessary.

Access to Latest Technology, Software and Development Tools
CSP's have a large suite of software applications and development tools. With SaaS the latest versions of software are made available to users as soon as they are released. CSP's also upgrade to latest technologies and hardware for building infrastructure as they have the resources and scale. Users have access to all these resources and can operate on the leading edge of technology and development tools.

Security
While Cloud certainly has security risks, it offers some security benefits as well. The CSP's take care of the software updates including security patches and updates and can deploy changes much faster and efficiently. This results in reduction of Mean Time to Patch (MTP) and Mean Time to Complete Changes (MTCC) security metrics [CIS 2010], reducing system vulnerability. Users thus worry less about security and can focus more on in its core purpose and goals.

1.3 Capacity v/s Utilization Curve

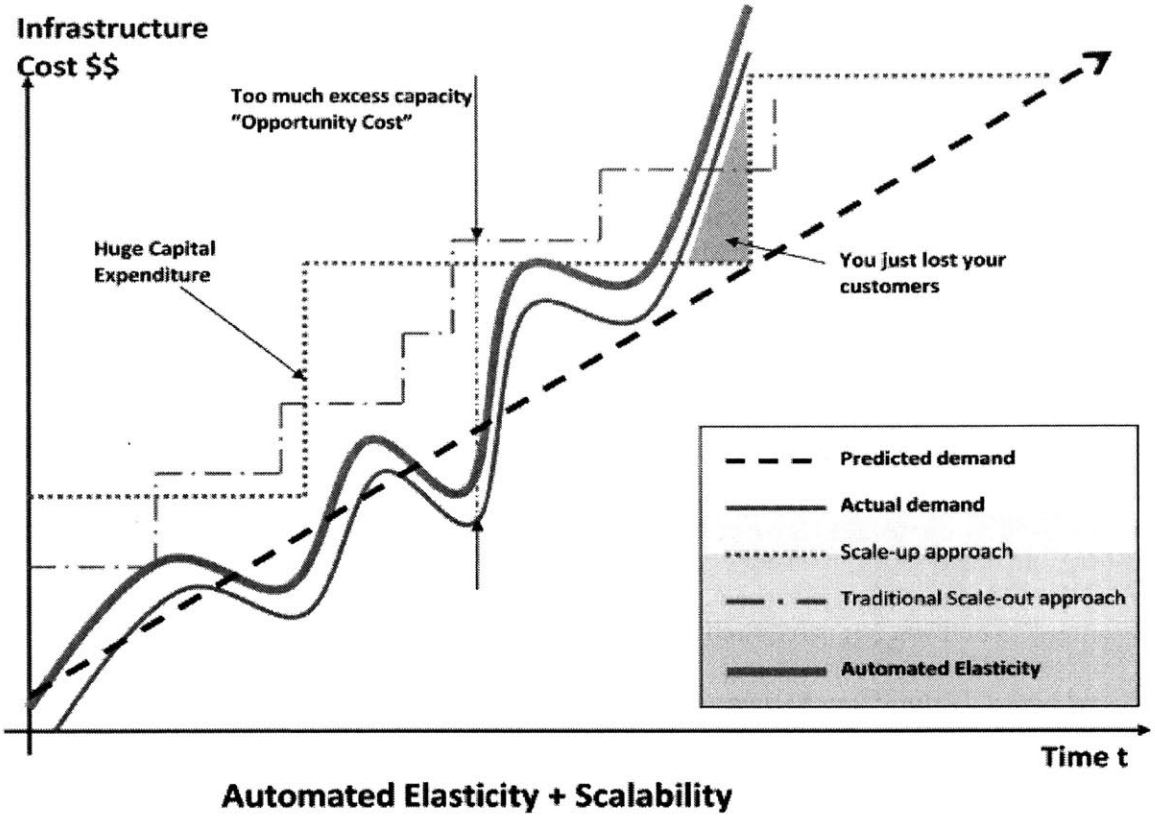


Figure 1.3: Automated Elasticity and Scalability [AWS 2011]

Figure 1.3 above by Amazon Web Services, shows the capacity v/s utilization curve. This model illustrates the central idea of having a utility based computing, with on demand access to resources to meet the actual demand. Traditional data centers require large capital expenditures and maybe underutilized if actual demand is low leading to opportunity cost. On the other hand, if actual demand is greater than capacity, then the business loses customers.

1.4 Barriers to Cloud Adoption

While cloud does provide enormous benefits to consumers, just like any other major technology, it comes with its own baggage of concerns and challenges. Some of the most important barriers to cloud adoption include [Wikipedia – Cloud Issues, SEI CMU]:

Security
Security remains by far the biggest barrier to cloud adoption. Users don't have control over their data or know where its stored. Cloud security and its ramification will be discussed extensively in the coming chapters and is the central theme of this thesis.

Interoperability
A universal set of standards for cloud technologies has not yet been defined, so there is a significant risk of vendor lock in. The high switching cost acts as a barrier to cloud deployment.

Limited Control and Autonomy
The users have limited control over the services and data. While the control and autonomy varies depending on the deployment model, it still is less than what a typical data center offers.

Latency and Performance
Cloud is delivered over the internet and there is additional latency introduced. The performance may be limited or inconsistent. However, companies like Amazon AWS are offering cloud delivery through dedicated lines for a premium [AWS DirectConnect].

Reliability
Many cloud computing providers use commodity hardware (servers, storage) which have limited reliability and are prone to failures. Additionally, the Service Level Agreements (SLA) for cloud are still evolving and are not standardized.

Platform or Language Specificity
Some cloud providers provided support for specific languages and applications only and are thus limited in their capabilities. However, the big players like AWS and Azure, provide a vast array of applications.

2: Motivation of Thesis and Background

"No problem can be solved from the same level of consciousness that created it." - Albert Einstein

Cloud computing is gaining increasing popularity and adoption and is one of the fastest growing technologies in present times. Cloud offers a lot of advantages in terms of economy of scale, flexibility, convenience but it raises major issues, especially loss of control of sensitive information and loss of security. As cloud computing is becoming increasingly pervasive, cybersecurity remains the principal concern among providers and subscribers alike.

2.1 Security Challenges in Cloud Computing

While cloud faces most of the cybersecurity risks that are applicable for any generic IT system, cloud computing provides additional security challenges and dimensions. Some of these are listed below [COSO 2013].

Lack of Transparency and Availability of Security Data
Depending on the type of cloud deployment (SaaS, PaaS, IaaS), the cloud customer may be unable to obtain security logs or operational data from the cloud solution provider. Thus it may be unable to be proactive or take measures against possible future attacks.

High Value Cyber-Attack Targets
Since the cloud contains consolidated data for several organizations which operate on the same infrastructure, it becomes a more attractive target for perpetrators. Instead of having to breach security of multiple individual organizations, they can just target the security of cloud.

Risk of Data Leakage
Since the same infrastructure houses data for multiple different organizations, the possibilities of data leakage increases and there is higher risk of losing data confidentiality or privacy.

System Availability
The system must be capable of continuing operations even in the possibility of a security breach. This includes both software and hardware resources. The cloud service provider (CSP) must guarantee that information is available and can be processed on demand even if the cloud infrastructure is breached.

IT Organization Issues
Another issue, in the context of socio technical systems is the morale and dedication of IT staff of the company. If a company migrates to cloud, the majority of the workload is handled by CSP leaving the in-house IT staff demotivated and they could assume that cybersecurity is the CSP's problem not theirs.

2.2 Migrating to Cloud – Security Issues

One of the major decision making points faced by CEO's/CTO's today are [CSA 2009, CSA 2011]:

- Whether to migrate to Cloud or not?
- If migrating to cloud, which deployment model to use (public, private or hybrid cloud)?
- Which delivery service to use (SaaS, PaaS, IaaS)?
- Which applications to migrate to Cloud?
- What are the Cloud Security Metrics?
- What are the risks associated?
- What's the ROI and does it make business sense?

While this problem is a daunting one and requires in depth analysis across the spectrum of organizations, and multitude of use cases, this thesis attempts to lay the ground work for this problem and identify some key decision points, which will help facilitate this decision and provide a starting point for discussing cloud migration.

Defining and measuring risk at a sufficiently granular level remains a key challenge. The thesis will evaluate existing prominent cybersecurity frameworks, threat metrics and models. By having a framework for evaluating or measuring cybersecurity risk, one can come up with either a qualitative or qualitative model to evaluate security features offered and calculate their ROI. The thesis will attempt to provide a preliminary framework for evaluating risk and ROI for migrating to cloud, with Target as a use case. By using this framework, CTO's can find recommendations to questions such as whether to migrate to cloud or not, which applications to migrate to cloud etc. Ultimately the answer to these questions depends on the particular company or organization, its specific needs, its appetite for Risk and ROI requirements.

Some of the topics discussed under this framework are

- Cloud Delivery Models and Security Requirements
- Major Cloud Computing Security Issues
- Cyber Risk and Risk Metrics
- Cybersecurity Frameworks, Threat Metrics and Models

Another topic discussed in this thesis is to find ways to manage and prevent Cyber-Attacks, which are becoming increasingly sophisticated. To understand and manage cybersecurity threats in today's complex and dynamic environment, a new approach is required to complement the traditional approaches to cybersecurity. While numerous frameworks and methods have been developed over the decades and are widely used, none of these are comprehensive enough to provide total immunity against cyber-attacks. These approaches try to solve some of the issues or shortcomings within the system while still leaving soft areas which end up getting exploited by hackers and compromise the IT systems.

Cyber threat is all pervasive and remains the single biggest threat to national security along with terrorism and corporations around the world are exposed to this menace. Cyber-attacks are getting

more sophisticated and audacious in their approach. Companies like TJX, Target and Home Depot, ended up losing hundreds of millions of dollars due to security breaches. More than the monetary value is the loss of customer information and privacy and the loss of perceived brand image of the companies.

Needless to say, prevention against cyber threats remains one of the key challenges of the CTO/CSO. To add to this daunting challenge, today's IT systems are the integration of a multitude of cutting edge technologies, in both hardware, software and applications. As we are migrating to 5G Wireless, to Internet of Things and Cloud Computing, with the rewards of fast connectivity, hundreds of always on, always connected devices and on demand computing, the fundamental landscape of cybersecurity is changing. Integrated Systems and having consolidated information on cloud, present an even bigger opportunity and rewards for hackers to look for ways to compromise these systems.

One requires to take a holistic approach to problem solving and understand the interrelationships and interdependencies of these complex socio technical systems. [Young 2014]. The System Theoretic Accident Model and Processes (STAMP) [Leveson 2011] approach which has its roots deep in Systems Theory believes that safety is an emergent property and incidents are the result of inadequate control. In this thesis, we attempt to apply STAMP approach to recent cybersecurity breach at Target and understand the effectiveness of this approach, specifically generating recommendations at both systemic and detailed level. By doing root cause analysis and identifying factors leading to the accident, we will also explore the possibility that whether migrating to cloud can alleviate some of the security threats and reduce certain attack vectors that a typical organization is exposed to. The lessons learnt from this analysis will help address the ongoing challenges in cybersecurity and help companies take measures and place sufficient controls in place to avoid security breaches.

2.3 Prior Literature Research

In this thesis, a variety of sources have been looked at including prior research papers, technical reports, research done by cloud and cybersecurity organizations such as Cloud Security Alliance(CSA) [CSA 2009, CSA 2011], Center for Internet Security(CIS) [CIS 2010] as well as standardization organizations such has National Institute of Standards and Technology (NIST) [NIST 2014, NIST-Metrics]. The next section will describe each of these sources and related work done in detail.

2.3.1 Cybersecurity Frameworks and Standards

National Institute of Standards and Technology (NIST)
The National Institute of Standards and Technology recently published a summary of observations from the Cybersecurity Workshop in April 2016 [NIST 2016]. NIST worked with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. NIST has also provided a cloud computing reference architecture as well as risk management framework. NIST has also done preliminary work in providing templates for Cloud Specific Service Level Agreements (SLA). It has also developed

recommended Security Controls for Federal Information Systems and Organizations [NIST-Metrics]. These frameworks will be referenced and used throughout the thesis, wherever applicable. We will apply some of the frameworks and security controls during STAMP analysis of Target Case and while also laying out the general framework for cloud migration in the context of cybersecurity.

European Union Agency for Network and Information Security (ENISA)

The European Union Agency for Network and Information Security has published a report on the benefits, risks and recommendations for cloud computing [ENISA 2009]. The publication has an extensive list of the key security risks areas classified into policy and organizational risks, technical risks, legal risks as well as risks not specific to the cloud but general cybersecurity risks. The work done by ENISA provides high level security benefits as well as risks and opportunities in cloud computing.

COBIT – Control Objectives for Information and Related Technology

The Control Objectives for Information and Related Technology (COBIT) is a framework created by Information Systems Audit and Control Association (ISACA) for IT management and governance. It provides a framework for IT managers to balance IT requirements, technical issues and business risks. However, COBIT does not naturally lend itself to causal analysis, so additional methods would need to be required after COBIT is implemented. COBIT also has complicated structure and concepts and is not easy to implement. Thirdly COBIT has ability to integrate with other standards which would require broader expertize in order to manage a multitude of integrated standards [Cyber Safety CISL, Hamid 2014, COBIT, COBIT 2013].

ISO/IEC

The International Standards Organization (ISO) and International Electro Technical Commission (IEC) jointly publish information security standard. This standard is comprehensive and provides the best security practices, based on learnings and experiences from previous events. However, the standards are not current and unable to keep pace with the rapid changes in cybersecurity threats [ISO, Cyber Safety CISL, Hamid 2014].

Cloud Security Alliance (CSA)

The Cloud Security Alliance [CSA 2011] provides security guidance for critical areas of focus in cloud computing. It identifies fourteen critical domains which represent both tactical and strategic security "pain points" within cloud and can be applied to any combination of cloud service and deployment model. It also provides broad guidelines on deciding what, when and how to move to the cloud. This is a very useful reference and provides broad recommendations, however it's very generic and lacks architecture specific details and quantitative framework to help facilitate data driven decision. CSA also has developed a framework for cybersecurity controls [CSA 2010]. They have established a working document with leading cybersecurity and cloud experts to identify the major security controls and map them to the various cloud deployment models and delivery services. These frameworks provide a useful starting point of discussion when a company is thinking about cloud migration and identifies the major areas of cybersecurity that it should be concerned with.

2.3.2 Cloud Security Metrics

Security remains the single most concern for mass adoption of Cloud Computing. The work done by European Union Agency for Network and Information Security [ENISA 2009] clearly identifies security and privacy as a major hurdle in the adoption of cloud. What makes the issue even more difficult to address is the lack of clearly defined and universally accepted security criteria and metrics against which to measure the various cloud computing platforms. The central question that needs to be addressed is to have a set of metrics by which one can objectively evaluate the security of a cloud and then decide whether it meets the organization's requirements.

The special characteristics of cloud; using the state of the art technologies and being a complex, evolving system, makes the problem even harder to solve. Several attempts have been made to define a structure and framework to address cloud computing security [Luna 2011]. This paper proposes the basic building blocks of proposed security metrics and attempts to classify requirements into three different sections, namely taxonomy, metrics and reference architectures. Notable work in taxonomy is developed by ENISA, Cloud Security Alliance(CSA)- Common Assurance Maturity Model (CAMM). Although not specific to cloud, National Institute of Standards and technology, NIST and Center for Internet Security (CIS) have done broad work in security taxonomies. The CAMM model [CAMM 2011] has done some foundational work in laying out metrics and measurements for Cloud Security but its work in progress.

2.3.2.1 Quantitative Risk Frameworks and Metrics

The research done by several authors [Brunette 2009, Latifa 2013], clearly identify security as the top threat to the mass adoption of cloud computing. They also classify the various kinds of cybersecurity threats as it pertains to cloud computing. This paper, among others can be used as a baseline to classify and identify major threats and devise corrective action against them.
In a complimentary paper, [Chow 2009, Latifa 2013], classify the security issues in cloud computing into three separate categories

- Cloud Provider-related vulnerabilities
- Availability of Service
- Data Control

Paul E. Black [Black 2009, Latifa 2013] discusses cybersecurity metrics in his book and the metrics define the extent to which the security controls are in compliance with procedures and policies. Incorrectly defined security metrics are often the bane of cybersecurity.

The previous work done by Jonsson and Pirzadeh [Jonsson 2011, Latifa 2013] differentiates security metrics into protective metrics, which reflects the ability of the system to protect itself from aggressors, and behavioral metrics, which define the operational attributes of the system. The paper proposes three security metrics

- Mean Time to Failure (MTTF)
- Mean Time to Catastrophic Failure (MTTCF)

- Mean Time to Repair (MTTR)

The Center for Internet Security (CIS) [CIS 2010] has proposed quantitative metrics to help organizations to make cost effective security decisions. These include 28 metric definitions across 7 business functions. Some of the metrics include Mean time to Incident Discovery (MTTID), Mean Time between Security Incidents (MTBSI), Mean Time to Incident recovery (MTIR), Mean Time to Complete Changes (MTCC) to name a few. These metrics together with the MTTR do provide a baseline for defining and measuring security risk however they have several shortcomings. Some of them being their effectiveness varies from one organization to the other, measuring the parameters might be infeasible and mean values might not be useful representation if the distribution of data is bi-modal or multi-modal.

Carnegie Mellon's Software Engineering Institute [COSO 2013, CMU 2010] have attempted to provide a taxonomy of cybersecurity risks. They have classified cybersecurity risks into four classes: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events. Each class is broken down into subclasses, which are described by their elements.

In the paper by Latifa [Latifa 2013], the authors explore a user-centered measure of cyber-security, and used this framework to analyze cloud computing as a business model. The authors present a quantitative framework to estimate the security of a system. The Mean Failure Cost (MFC) metric is used to provide the failure cost per unit time (e.g. $/hour) and quantify the impact of security failures. It also distinguishes between different stakeholders and provides cost for each stakeholder depending on its threat level and damage due to breach of information. This paper defines cloud security in economic terms enabling various stakeholders to quantify their risks and take decisions based on ROI. It also captures the complexity and heterogeneity of cloud computing systems. However, this framework assumes generic architecture for cloud computing and hence may not be applicable to specific Cloud architectures like AWS or Azure.

2.3.2.2 Qualitative Risk Frameworks and Metrics

The qualitative risk based security frameworks are described below:

OCTAVE
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is developed by the Software Engineering Institute of Carnegie Mellon University [OCTAVE CMU, Mayer 2009] is an approach used to assess an organization's information security needs. Octave can be used in a collaborative setting to perform risk assessment without extensive organizational involvement. OCTAVE Allegro, based on the two older versions of OCTAVE called OCTAVE Original and OCTAVE-S (simplified) is the most recently developed and actively supported method. It is a more comprehensive version for large organizations or those with multilevel structures. OCTAVE Allegro consists of eight steps organized into four distinct phases:

- Developing risk measurement criteria consistent with organizations mission and objectives
- Create a profile for each critical information asset with clearly defined boundaries

- Identify threats to each information asset
- Identify and analyze risks to information assets and develop counter measures.

OCTAVE is a qualitative framework; hence its effectiveness may be limited. It's hard to quantify security risks using this framework and organizations may find it difficult to prioritize or rank order risk because of lack of inherent processes.

CRAMM

CRAMM (CCTA Risk Analysis and Management Method) is another qualitative risk analysis and management tool, developed by UK Government's Central Computer and telecommunication Agency (CCTA) in 1985. CRAMM has had multiple revisions since then and evolved into a widely accepted methodology in use by both defense agencies and corporations alike [Mayer 2009, Latifah 2013].

CRAMM has three distinct phases:

- The establishment of the objectives for security
- The assessment of the risks
- The identification and selection of countermeasures

Apart from being a qualitative framework, CRAMM requires need for very experienced practitioners to be effective. The full reviews may last too long, which may be ill suited to the rapid pace required to counter today's cybersecurity threats. Both OCTAVE and CRAMM have a "Low/Medium/High" classification of risk assessment rather than more granular and specific value. They also do not distinguish between stakeholders or provide a dollar value associated with a particular risk or threat.

2.3.3 Failure/Accident Models in Cybersecurity

The section below discusses some of the prominent frameworks for analyzing failures or accidents in traditional cybersecurity environments. While cloud has additional complexity due to a different architecture, many of these frameworks can also be adapted to analyze failures in cloud.

2.3.3.1 Linear Chain of Events Model

The first generation accident models attributed cause of an accident to a single risky behavior or circumstances which lead to that risky behavior. As accidents became more sophisticated, the second generation models evolved to incorporate multiple causal factors or events which led to the accident [Cyber Safety CISL, Hamid 2014, Leveson 2011].

The linear chain of events model describes accidents in terms of multiple events, sequenced as a forward chain over time, chronologically. The objective of this model is to manage or eliminate risk of an accident by implementing sufficient controls or counter measures in between the events in the chain so as to break the sequence. This model is relatively simple to construct and causal factors can be easily identified.

There exists a simple, direct relationship between events in chain and it ignores the nonlinear relationships among events or feedback etc. Also events almost involve component failure, human error or an energy related event. Therefore, preventing the lowest level event and achieving higher reliability became the center point of linear chain of events model.

There are several fundamental limitations of Linear Chain of Event Model, some of them are listed below

- It focuses only on component reliability.
- It cannot access software design errors.
- It cannot capture, social, organizational and economic factors of the accident.
- It cannot represent system change over time.

2.3.3.2 Fault Tree Analysis

Fault Tree Analysis [Cyber Safety CISL, Hamid 2014, FTA] is a top down, deductive failure analysis in which a faulty state of the system is analyzed by using Boolean Logic to combine a series of low level events. FTA creates a logic diagram of the entire system and maps the relationships between faults, subsystems and safety design elements. It thus enables a high level understanding of the system allowing for quick detection of faults or hazards within the system. However, it also has severe limitations, in addition to the limitations of Chain of Events Model,

- It is not good at finding all possible initiating faults.
- Constructing a tree requires detailed understanding of the system design and operation, otherwise a generic tree will not be that effective.
- In a complex cyber system with many sub systems or proprietary subsystems or software, FTA can only be used for verification of systems which are in full control of the operator.
- For software systems, FTA also requires detailed documentation of software logic in order to be effective, which can be a challenge.

2.3.3.3 Cyber Kill Chain

The Cyber Kill Chain framework is defense driven model for the identification and prevention of cybersecurity intrusions. The model identifies what the attackers must accomplish in order to achieve their mission. the concept of breaking an adversaries Kill Chain is a method of preemptive action. The Kill Chain method consists of seven distinct phases. These are described in Figure 2.3. More recently, the Cyber Kill Chain framework has been adopted by Lockheed Martin to model intrusion of a computer network. The "Kill Chain" is originally a military concept dating back a long time and breaking an opponent's Kill Chain is to pre-emptively defend oneself against the attack. Although it's a compelling framework, it too has several shortcomings, mainly narrow focus on perimeter based malware prevention thinking. Also, the scope of today's cybersecurity threats far extends beyond the Cyber Kill Chain. A motivated and persistent attacker, will always find a way around the Cyber Kill Chain and venture into the opponent's network unobstructed [Kill Chain 2014, KC CSO, KC 2014].

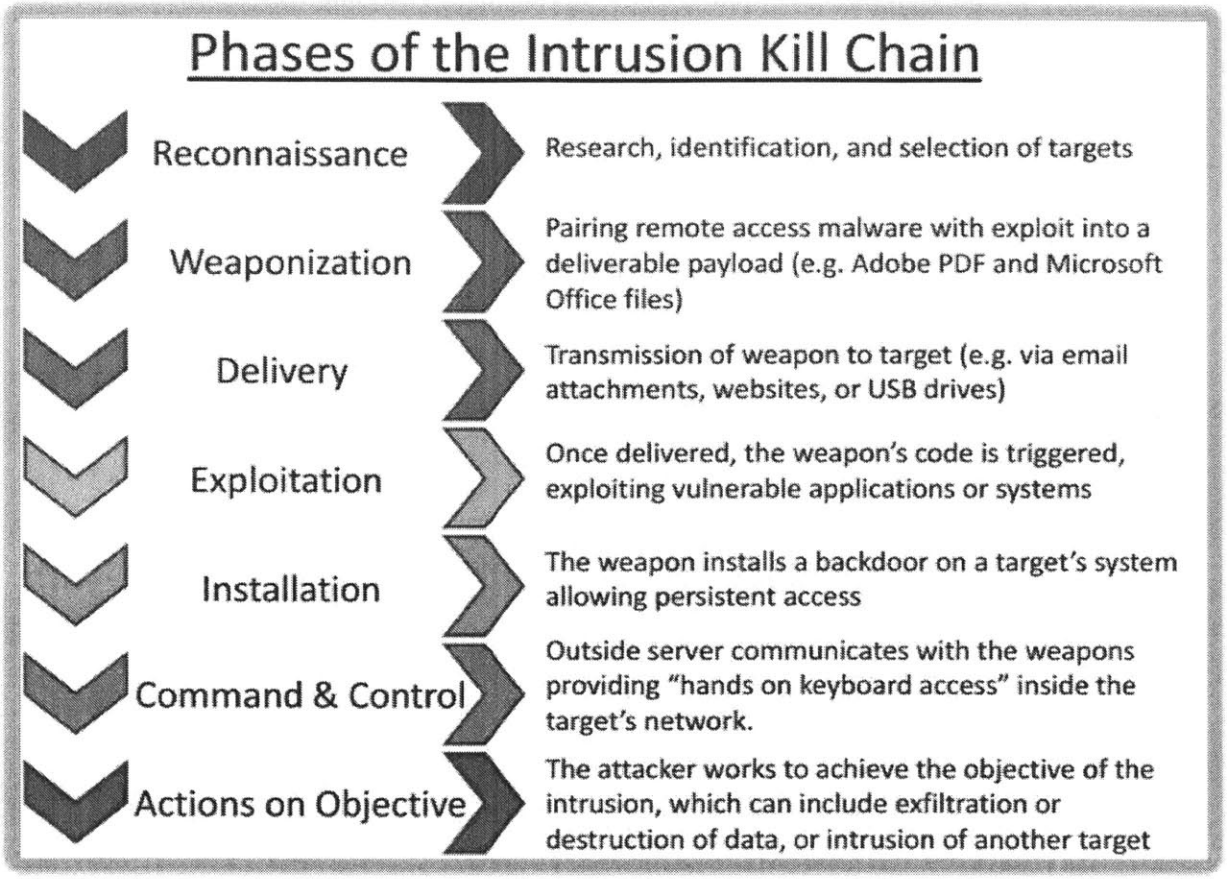


Figure 2.3 Phases of the Intrusion Kill Chain [Kill Chain 2014]

2.3.3.4 System-Theoretic Accident Model and Processes - STAMP

It's obvious that although the various frameworks and methodologies help in identifying parts of the problem, they lack innovation and don't guarantee immunity from cybersecurity threats. Most of these models attempt to lay a security perimeter around the technology assets of the organization. On the contrary, the threats of cybersecurity increase every day as hackers are becoming more sophisticated in their approaches and always find ways to break into the system. Today's IT systems are complex and dynamic and require a new approach to problem solving, including the socio technical aspects of the system. These are complex system of systems and require holistic approach to defend against possible cyber-attacks. One model, rooted in Systems Thinking and Systems Theory is called System-Theoretic Accident Model and Processes (STAMP). This model has been developed by Prof Nancy Leveson at MIT [Leveson 2011, Leveson STAMP 2004]. STAMP has been successfully applied to a variety of projects including those at NASA [Leveson NASA] and US Ballistic Missile Defense System. [Pereira STAMP]. STAMP can also be applied to Cyber Physical Systems (CPS) and recently it was applied to Stuxnet cyber-attack [Arash Madnick]. This paper is the first STAMP based analysis of a major

CPS attack and it identified a threat that was not exploited by Stuxnet virus. STAMP methodology has also been applied to TJX security breach and generated promising results and recommendations as part of the analysis [Cyber Safety CISL, Hamid 2014]. The lessons learnt from the analysis can be applied to other major security breaches like the Target security breach of 2013. While none of the approaches is complete, STAMP does require a holistic view [Young 2014] of problem solving and looks at multiple dimensions including technology, people, processes, management support among others.

2.4 Thesis Structure

This thesis will attempt to address several open issues. Firstly, it will attempt to evaluate several security controls, metrics and frameworks for cybersecurity in general and cloud in particular. It will define a cloud migration decision framework that companies can use as a starting point to guide their decision process. It will then apply the Systems Thinking framework, specifically STAMP failure/accident model to Target case and identify the major causal factors as well as a list of recommendations. It will finally apply the cloud migration framework to Target and evaluate whether migrating some applications to cloud can help reduce the threat profile for some companies.

2.4.1 Cloud Migration Framework

Whether enterprises should migrate to cloud or not and what are the key security ramifications remains a challenging decision for many CTO's. While different frameworks, models and metrics have been proposed, there is no well-defined guideline to help organizations make this decision. This decision is complex as it involves balancing the needs and requirements of multiple stakeholders, evaluating risks and ROI and often times take decisions without having access to all necessary information as its controlled by the cloud provider. To add to the decision complexity, there are different cloud delivery and deployment models, a host of Cloud Service Providers (CSP), with, different architectural implementations and security features. This leads to many permutations and security risks vary according to the chosen profile.

2.4.2 Failure and Accident Analysis of Target Data Breach using STAMP Framework

Secondly, the traditional failure/accident models are not sufficient in preventing or analyzing cyber-attacks. These attacks are becoming increasingly prevalent and sophisticated. These issues are extremely complex problems with no easy or straightforward answers. The traditional engineering approaches and analysis which focuses on individual pieces of the problem and tries to fix things has proven to be inadequate. These problems involve multiple stakeholders, are recurring problems and are a result of a complex interactions among the system and with the larger environment at large. Systems Thinking, which is the process of understanding how those things which may be regarded as systems influence one another within a complete entity, or larger system is a powerful approach to solve some of the security problems of complex systems like cloud computing infrastructure. The Systems Thinking approach is ideally suited to solve such problems and having a big picture view of the problem space. Cloud computing also adds extra dimensions

in cyber threats and remains one of the critical challenges in widespread adoption of cloud computing.

One requires to take a holistic approach to problem solving and understand the interrelationships and interdependencies of these complex socio technical systems. The System Theoretic Accident Model and Processes (STAMP) approach has its roots deep in systems theory believes that safety is an emergent property and incidents are the result of inadequate control [Cyber Safety CISL, Hamid 2014]. In this thesis, we shall apply the STAMP framework [Leveson 2011, Leveson STPA] which is based on Systems Thinking, to Target data breach and identify the causal factors that led to the accident and also come up with list of recommendations based on the analysis. The lessons learnt from this analysis will help address the ongoing challenges in cybersecurity and help companies take measures and place sufficient controls in place to avoid security breaches. We will also attempt to develop a framework for cloud migration with emphasis on cybersecurity controls and security metrics.

2.4.3 Applying Cloud Migration Framework to Target Case

Finally, we shall apply the Cloud Migration Framework to Target and identify applications which could potentially be migrated to cloud. We shall evaluate which cloud delivery models and service model would make sense for migration. We will evaluate the decision in the context of cybersecurity and answer the question whether moving some applications to cloud could avoid some of the Threat Vectors and reduce risk profile. Would companies like Target reduce their cybersecurity risks if they migrate non critical systems to the cloud remains an interesting question to be addressed. Companies can potentially leverage the cost and security benefits of cloud allowing them to focus on securing key and strategic data and applications. This can help reduce some attack vectors and isolate critical systems. Providers can also explore using IaaS and using virtualized systems in a secure private cloud. There are tradeoffs in each of these decisions and the thesis will attempt to explore and evaluate some of these alternatives.

3: Different Types of Cloud Deployment Models and Delivery Services

"The first veil to vanish is ignorance; and when that is gone, unskillful behavior goes; next desire ceases, selfishness ends, and all misery disappears." - Veils of Maya, Upanishads, Vyasa Sutra

3.1 Cloud Deployment Models

There are different kind of cloud deployment models [Wikipedia – Cloud, CSA 2009]. Each of these models have different characteristics and offer varying degrees of security, reliability, performance, as well as cost. A cloud user needs to evaluate its requirements especially in terms of security and risk tolerance and then decide which cloud deployment best meets its needs. Some of the main cloud deployment models are described below.

3.1.1 Public Cloud

A cloud is referred to as "Public Cloud" when its services are rendered over a network for public consumption. Although technically there may be little difference between public and private cloud, the security ramifications between the two may be substantial for various services (applications, storage or other resources). Generally public cloud service providers like Amazon Web Services (AWS) and Microsoft operate their own cloud infrastructure and deliver services via public internet. AWS and Microsoft Azure also provided more secure direct connect services, which requires customers to buy or lease private connections for using cloud services, however they are still not as secure as private cloud.

3.1.2 Private Cloud

A cloud is referred to as "Private Cloud" when its services are rendered for a single organization, whether it's hosted internally or by a dedicated third party and hoisted within the organization or externally. Running a dedicated cloud requires significant commitment of resources and time and high level of engagement. It also requires significant capital expenditures. It may host single tenant or larger enterprises may use multi tenancy to provide access to different business units, departments or locations. Private cloud is under direct control of the organization and thus offer higher level of control and performance along with other benefits as that of Public Cloud. Also typically private cloud is more secure than public as some of the major security threats in cloud (full list discussed in later chapters) such as data leakage (due to multitenancy) are less of a concern.

3.1.3 Hybrid Cloud

A Hybrid Cloud is the amalgamation of two or more clouds (public, private or distributed etc.) that remain distinct entities but are bound virtually to form one cloud so as to be indistinguishable. Hence they offer benefits of multiple deployment models. A hybrid allows one to extend the

capacity or capability of a cloud service. There are different use cases of a cloud service. For e.g. an enterprise may decide to migrate the highly sensitive information (e.g. customer passwords, IP) on a private cloud, while use public cloud for software development. Another use case might be to use private cloud as default configuration and move to public cloud during peak traffic when temporary capacity is required. Hybrid cloud must enable data and application portability and can even support different CPU architectures (e.g. x86 and ARM).

3.1.4 Managed Cloud or Community Cloud

This type of cloud is a collaborative effort among several organizations who form a community and have similar concerns (security, compliance etc.) The costs are spread over fewer users (compared to a public cloud). Community clouds offer similar benefits as public cloud in terms of scalability and cost with added benefits of greater control over domains that are critical to members of the community.

3.1.5 Others

There are also other types of cloud models though not that common in practice currently. Some of these include "distributed cloud", which is a cloud computing platform assembled from a distributed set of machines in different physical locations [Wikipedia – Cloud]. InterCloud is an interconnected global "cloud of clouds" which allows interoperability between public and private cloud service providers. Finally, multicloud is another type of cloud model which offers multiple cloud computing services in a heterogeneous architecture. For e.g., an enterprise may use different cloud service providers for Infrastructure as a service (IaaS) and Software as a Service (SaaS) or even use different providers for IaaS.

3.2 Cloud Deployment Models – Key Characteristics

The key characteristics of the main three cloud deployment models (public, private, hybrid) are described in Table 3.2 below.

Characteristic	Public cloud	Private cloud	Hybrid cloud
Scalability	Very high	Limited	Very high
Security	Good, but depends on the security measures of the service provider	Most secure, as all storage is on-premises and greater control and autonomy	Very secure; integration options add an additional layer of security
Performance	Low to medium, but d	Generally Very good	Good, as active content is cached on-premises
Reliability	Medium; depends on Internet connectivity and service provider availability	High, as all equipment is on-premises	Medium to high, as cached content is kept on-premises, but also depends on connectivity and service provider availability
Cost	Very good; pay-as-you-go model and no need for on-premises storage infrastructure	Good, but requires on-premises resources, such as data center space, electricity and cooling	Improved, since it allows moving some of storage resources to a pay-as-you-go model

Table 3.2: Characteristics of Different Types of Cloud Deployments [TechTarget]

3.3 Cloud Delivery Services

Though the holy grail of service oriented architecture is "everything as a service" or EaaS/Xaas, [Wiki – EaaS] cloud computing providers offer services through three main models, each of which represents a different part of the cloud computing stack [Wikipedia – Cloud].

3.3.1 SaaS

The Software as a Service or SaaS provides the customer the ability to run the cloud provider's software on the cloud infrastructure. The cloud providers manage the underlying infrastructure and platforms that run the various applications and the user does not have much control with the exception of the application configuration. Usually these applications are provided through thin client interface and are billed as pay per use or a subscription. Big cloud providers like AWS and Microsoft Azure offer an extensive range of software offering as part of SaaS. Security for the most part in SaaS is the responsibility of the CSP. The CSO needs to focus mainly on the user access to the applications.

3.3.2 PaaS

The Platform as a Service or PaaS offers a development environment to application developers. The cloud provider provides the capability to deploy consumer created or third party applications onto the cloud. They provide a development environment which typically includes the operating system, databases, programming languages and web server. The customer does not have control over the underlying hardware, servers, storage, network or operating system but controls the application and its different configurations. Thus PaaS provides one level higher abstraction than IaaS. While the CSP is responsible for securing the infrastructure, the customer is responsible for the security and control of the applications. Some of the popular PaaS platforms include AWS Elastic Beanstalk, Windows Azure, Heroku, Google App Engine and Apache Stratos.

3.3.3 IaaS

The Infrastructure as a Service or IaaS contains the basic building blocks for cloud IT and provides the consumers with the fundamental resources in computation, networking, and data storage. This is the closest to a self-managed data center and the customer can run any Operating System and applications using IaaS. IaaS provides flexibility and management control over IT resources. In this model, the CSP is only responsible for the security of the underlying infrastructure and resources, while the onus for integration, securing applications and data is the responsibility of the consumer. Some examples of IaaS include Amazon EC2, Windows Azure, and Google Compute Engine.

3.4 Inherent Risk and Control Relationship of Cloud

The risks and level of control varies according to the deployment and delivery models (illustrated in Figure 3.4). As we move from Private to Public Deployment Model, the degree of inherent risk that the user is exposed to increases and as we move from IaaS to SaaS Delivery Model, the level of control decreases. Figure 3.4 assumes an inverse relationship between control and inherent risk., i.e. as control decreases the risk profile increases. The actual risk profile depends on the CSP and its particular offering. For e.g. a SaaS offering by one of the major cloud providers could actually offer a very high level of security compared to traditional IT as the CSP has the resources and scale to implement a variety of security controls and features.

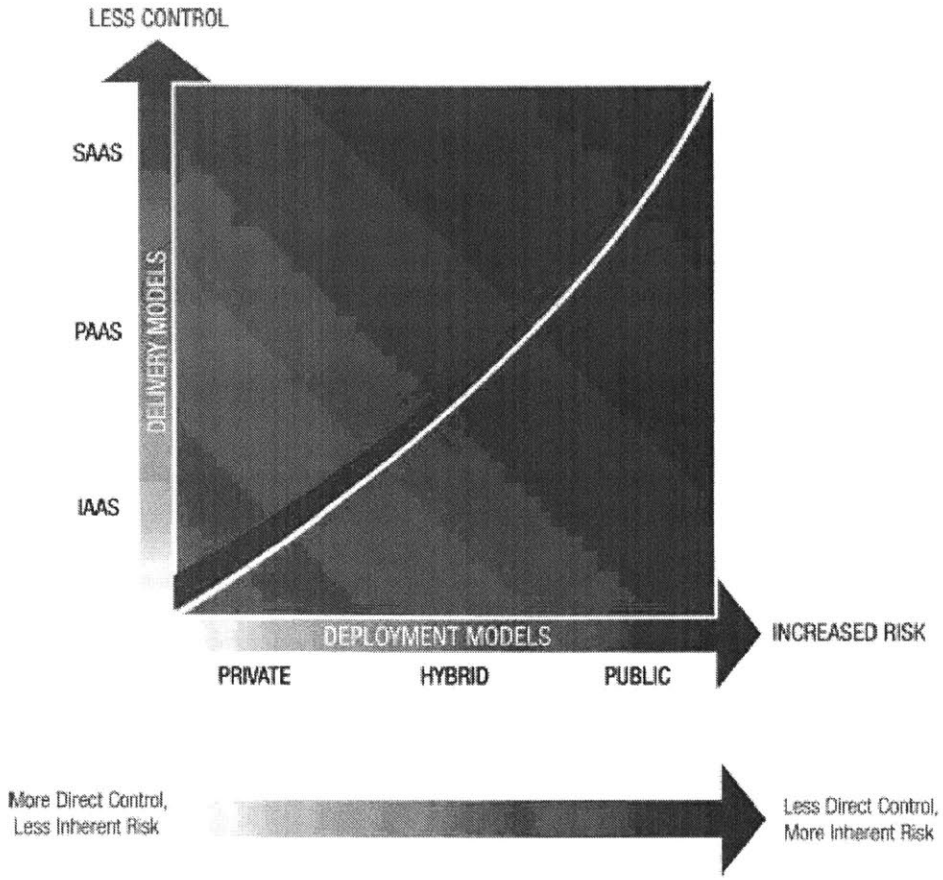


Figure 3.4: Inherent Risk Relation of Cloud Service Delivery and Deployment Models [COSO 2013]

4: Cloud Computing Security Issues and Benefits

For all your days prepare And meet them ever alike. When you are the anvil, bear - When you are the hammer, strike." — A.P.J. Abdul Kalam, Wings of Fire

4.1 Cloud Computing Security Issues

While many companies including both in the public and private sector are thinking of migrating to cloud, security remains the top threat in the large scale adoption of cloud. [CSA 2010]. While enterprises are migrating parts of their business to cloud, security remains a top concern. The first important step in minimizing risk in cloud is to identify top security threats.

The Cloud Security Alliance (CSA) has done extensive work in this area and listed the following top security threats to cloud computing [CSA 2010]. The on demand and shared nature of cloud computing does introduce new threat vectors which to an extent erases gains made by switching to cloud technology. While some of the security threats are similar to what a typical IT data center is exposed to, several new threat vectors are introduced and the severity of some of the threats increases due to the characteristics of the cloud (e.g. multitenancy, resource sharing)

The top security threats in cloud computing identified by CSA [CSA 2016] are listed below.

4.1.1 Data Breaches

Since cloud servers host massive amounts of data for a large number of customers, they become an attractive target for malicious attackers. Cloud can not only contain financial information data, but also personal healthcare information and intellectual property. A data breach exposes cloud vendors to lawsuits and fines and rack up significant costs. Loss of reputation and trust by customer can also significantly add up to the expenses. While cloud providers deploy security controls for every kind of service and deployment model, ultimately the onus for secure data is on the customer. CSA recommends multifactor authentication and encryption to protect against these attacks.

4.1.2 Compromised Credentials and Broken Authentication

Data breaches are often a consequence of lax authentication, weak passwords and poor key or certificate management. Sometimes organizations forget to remove user access when a person leaves the organization or a job role changes. Developers sometimes leave their cryptographic key and credentials in the source code and leaving them in public repositories like GitHub. Multifactor authentication and establishing and maintaining a secure public key infrastructure does help in mitigating such attacks. Organizations which are planning to centralize identity within a single repository within a cloud, need to evaluate the security measures the CSP provides to protect the identity platforms.

4.1.3 Hacked Interfaces and API's

API's are provided by almost every cloud services provider. Cloud customers use API's to interact with cloud services including those to manage, orchestrate and monitor different services provided. The security of API's is very critical in maintaining the security and availability of cloud service. Sometimes third party builds on these interfaces using API's resulting in organizations having to expose more services and credentials and consequently exposing it to host of security issues related to confidentiality, integrity, availability and accountability. API's tend to be the most exposed part of the system because they are accessible on internet. Sometimes programmers who code the API's do not keep security in mind and can risk putting both the application and the underlying data at risk. API code which is not written with security in mind can add to the risk profile. The code should be audited by a security expert for vulnerabilities which can be exploited by a malicious attacker.

4.1.4 Exploited System Vulnerabilities

System vulnerabilities have become a bigger problem in cloud due to multitenancy. Organizations share resources such as memory, databases in close proximity to one another, creating new threat vectors. Protection against these vulnerabilities can however be done using basic IT processes such as patch management, vulnerability scanning and follow up on reported system threats. According to CSA, the costs of mitigating system vulnerabilities are relatively low compared to other IT expenses, however as architectures are still not standardized, the actual expenses depend on the particular CSP's implementation of the cloud. CSP's need to have efficient patch management systems and remediation activities documents in place as the cost to discover and repair vulnerabilities is small compared to the potential damage due to breach.

4.1.5 Account Hijacking

Threats to regular IT systems such as phishing, fraud and software breaches are all relevant to cloud with an added dimension to the threat because attackers can eavesdrop on activities, manipulate transactions and modify data. Attackers can also use the cloud to launch other attacks. The recommended strategy is securing account credentials and implementing a defense in depth protection strategy.

4.1.6 Malicious Insiders

This is another important threat to cloud services, since a single malicious insider can compromise the whole infrastructure or manipulate data. The threat can come from an employee, system administrator or a contractor. Systems which rely totally on cloud services provider for security have the greatest exposure to this risk. The recommended strategies by CSA include segregating duties and minimize access to users as well as using encryption process and keys. Other controls include effective logging, monitoring and auditing administrator activities.

4.1.7 The APT Parasite

The Advanced Persistent Threat (APT) systems are "parasitical form of attacks" [Ref CSA] and they infiltrate systems to establish a foothold and then exfiltrate data stealthily over time. APT's also move laterally within the network, masking their movements with regular traffic, making it hard to detect them. While CSP provides security controls to detect APT's, the customers too must be diligent in detecting APT compromises in cloud.

4.1.8 Permanent Data Loss

While this type of vulnerability has become increasingly rare, malicious hackers have been known to permanently erase cloud data to harm businesses. Cloud data centers are also vulnerable to natural disasters. To mitigate permanent data loss, the recommended strategy is to distribute data across multiple data zones as well as also keeping data backup and adhering to best practices in business continuity and data recovery. The downside of data replication is providing additional opportunities for stealing data.

4.1.9 Inadequate Diligence

Organizations who migrate to cloud should perform due diligence and fully understand the environment and the risks associated with it otherwise it can expose itself to a myriad of financial, legal, technical and compliance risks. For e.g., organizations must do due diligence of SLA to understand the provider's liability in case of data loss or breach

4.1.10 Cloud Service Abuses

Attackers can use cloud services and use the resources to launch an attack. Examples include launching DoS attacks, sending spam and phishing emails and hosting malicious content. Cloud providers need to scrutinize network traffic and develop tools that allow customers to monitor the health of their cloud environments. Providers should also offer a mechanism for reporting abuse.

4.1.11 DoS Attacks

A Denial of Service (DoS) attack is an attempt to make the network or computing resources unavailable to its users, such as temporarily disrupting or suspending services. A distributed denial of service (DDoS) is an attempt to make an online service unavailable by overwhelming it with attacks from multiple compromised systems. DoS attacks have been in existence for a while and they affect cloud computing by affecting availability of cloud services or resources. These attacks consume large amounts of computing resources, resulting in slow or no service and ultimately resulting in customer paying the cost of these attacks. Cloud providers have greater resources to handle DoS attacks and they should have a plan to mitigate the attack before it occurs, so administrators have access to all required resources in the event of such an attack.

4.1.12 Shared Technology, Shared Dangers

While shared technologies, infrastructure, platforms and applications in cloud bring great benefits, it also poses significant threats. A single vulnerability or misconfiguration in the system can potentially compromise the entire provider's cloud. If a shared platform component or an application gets compromised, it risks exposing the entire cloud environment to outside attacks. CSA recommends defense in depth strategy, including multifactor authentication at all hosts, intrusion detection systems, network segmentation and providing account privileges only as necessary. Each user needs to evaluate these security risks of shared technologies and factor in the cost of including the additional security measures before making a decision.

4.2 Recommended Security Countermeasures

The list of these top security threats and recommended risk mitigation strategies [CSA 2016] is given Table 4.2 below:

Threat	Counter Measure
Data Breach	Multi factor authentication and encryption
Compromised Credentials and Broken Authentication	Multifactor authentication and secure public key infrastructure
Hacked Interfaces and API's	Implement safety controls, threat modelling of applications and systems
Exploited System Vulnerabilities	Patch management, vulnerability scanning and follow upon on reported system threats.
Account Hijacking	Defense in depth strategy, securing credentials
Malicious Insiders	Effective logging, monitoring and auditing administrator activities. Segregating duties and minimize access to users as well as using encryption process and keys
Advanced Persistent Threats	Regular awareness programs, training on phishing activities, keeping upto date on latest security attacks
Permanent Data Loss	Regular data backup, distribution of data across multiple time zones, adhering to best practices
Inadequate Diligence	Perform due diligence and understand risks
Cloud Services Abuses	Providers must monitor network traffic for DDoS attacks, provide tools to monitor health of cloud environment
DoS Attacks	Plan to mitigate such attacks before they occur
Shared Technology, Shared Resources	Defense in depth strategy, including multifactor authentication at all hosts, intrusion detection systems, network segmentation and providing account privileges only as necessary

Table 4.2: Top Security Threats in Cloud Computing and Recommended Countermeasures [CSA 2016]

4.3 Cloud Security Control Domains

To aid both consumers and cloud providers, CSA has developed "Security Guidance for Critical Areas in Cloud Computing". This guideline has become the benchmark for best security practices in Cloud Computing. CSA has identified 14 Critical Domains of Security [CSA 2011].

These 14 Critical Domains are briefly described below. For more details, please read the "Security Guidance for Critical Areas of Focus in Cloud Computing" report by CSA [CSA 2011]

Domain 1: Cloud Computing Architectural Framework
This domain provides a conceptual framework for the rest of CSA's guidance. It describes cloud computing framework which is specifically tailored to security and network professionals. Understanding the architectural framework is critical for understanding the remainder of the domains. This domain also describes the various deployment models of cloud (Public, Private, Hybrid, Community etc.), Service Models (SaaS, PaaS, IaaS) and well as essential characteristics of Cloud (On Demand Service, Elasticity, Broad Network Access etc.). The rest of the thirteen domains highlight the critical areas of concern for cloud computing regarding both strategic and tactical security issues within cloud environment. Domain two to six deal with Governance issues in cloud whereas domain seven to fourteen deal with operations.

Domain 2: Governance and Enterprise Risk Management
This domain deals with the ability of the organization to govern and measure enterprise risk introduced by migration to cloud. Items such as legal precedence for agreement breaches, adequately access and measure risk and how international boundaries may affect such issues are some of the topics of concern in this domain.

Domain 3: Legal and Electronic Discovery
This domain deals with the potential legal issues such as protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws etc.

Domain 4: Compliance and Audit
Compliance and Audit domain deals with maintaining and providing compliance when using cloud services. This domain provides guidance on evaluating how cloud computing affects compliance its internal security policies as well as various legislative and regulatory requirements.

Domain 5: Information Lifecycle Management
This domain deals with data management in cloud and issues surrounding the identification and control of data as well as implementing controls for compensating for lack of physical controls when moving data to cloud. Also assigning responsibility for data confidentiality, integrity and availability are also discussed.

Domain 6: Portability and Interoperability
This domain discusses the ability to move data or services from one provider to another or transfer it back to in-house data centers. The important feature of interoperability in cloud is discussed.

Domain 7: Traditional Security, Business Continuity and Disaster Recovery
This domain deals with how cloud computing affects operational processes and procedures currently used to support security, business continuity and disaster recovery. Evaluating both the security risks as well as security benefits offered by cloud are also discussed.

Domain 8: Data Center Operations
The data center operations deal with how to evaluate cloud provider's data center architecture and operations and also identifying characteristics which could be detrimental to ongoing services as well as characteristics essential for long term security.

Domain 9: Incident Response, Notification and Remediation
This domain deals with proper detection, response, notification and remediation of cloud incidences. It helps bring to notice the complexities associated with handling incidents associated with cloud.

Domain 10: Application Security
This domain deals with important issues such as whether to migrate or design an application to run on cloud and if so which cloud computing platform to use (SaaS, IaaS, PaaS). Specific related security issues are also discussed.

Domain 11: Encryption and Key Management
This section deals with identifying proper encryption usage and scalable key management and also discusses why they are required as well as issues that arise while implementing them.

Domain 12: Identity and Access Management
This domain provides insight into and assessing an organization's readiness to conduct cloud based IAM. The emphasis is on issues that arise when an organization extends its identity into cloud.

Domain 13: Virtualization
This domain deals with the issues and risks that arise with virtualization. Items such as risks associated with multi-tenancy, VM isolation, hypervisor vulnerabilities are also discussed.

Domain 14: Security as a Service
Lastly, this domain has been the most recent entrant into CSA's list of critical domains and addresses the critical need of standardizing security in cloud which provides benefits to both users and CSP's. In the context of cloud security, a standardized security framework takes the form of document that specifies which security features are provided and under what conditions. There is a shared responsibility between CSP and the user. This domain provides third party facilitated security assurance, incident management, compliance attestation, and identity and access oversight. Security as a service delegates detection, remediation, and governance of security infrastructure to a trusted third party which has the proper resources and expertise. Security as a Service (SecaaS) [CSA 2011]is slowly maturing and getting adopted on a global scale. The

expectation is that a standardized security framework will eventually minimize the variances and voids in cloud security.

While developing the security risks and guidelines, The CSA [CSA 2011] has complimented and extensively referenced this research done by European Network and Information Security Agency [ENISA 2009]. ENISA has done a comprehensive study on risk management of cloud computing and contains several key recommendations. Table 4.4 below maps the top cloud security threats to the security domains and the service platform as well also recommending mitigation strategies for each security threat.

4.4 Mapping of Security Threats to Security Domains and Service Platforms

Table 4.4 below lists the top 7 Security Threats identified by CSA and maps them to the different Security Domains and effected Deployment Models. For a more comprehensive details on examples of each type of threat and the mitigation methodologies, please refer to CSA's publication [CSA 2010].

Threat	Domain	Service Platform		
		SaaS	PaaS	IaaS
Abuse and nefarious use of cloud computing	Domain 8 Domain 9		Yes	Yes
Insecure Interfaces and API	Domain 10	Yes	Yes	Yes
Malicious Insiders	Domain 2 Domain 7	Yes	Yes	Yes
Shared Technology Issue	Domain 8 Domain 13			Yes
Data Loss or Leakage	Domain 5 Domain 11 Domain 12	Yes	Yes	Yes
Account or Service Hijacking	Domain 2 Domain 9 Domain 12	Yes	Yes	Yes
Unknown Risk Profile	Domain 2 Domain 3 Domain 8 Domain 9	Yes	Yes	Yes

Table 4.4: Top Security Threats in Cloud mapped to Security Domains and Service Platforms [CSA 2010]

4.5 Security Benefits of Cloud

While the security risks associated with cloud computing have been discussed in great detail in literature, it's equally important to discuss the security benefits that cloud computing can contribute towards. Some of the main security benefits of cloud are discussed below [ENISA 2009]:

4.5.1 Security and Benefits of Scale

Security measures are simply cheaper when they are implemented on scale. Therefore, for the same amount of investment in security, cloud can offer better protection. All kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, vetting of human resources, strong authentication etc., can all be provided on scale, making them cheaper and efficient to implement. Large cloud providers such as Amazon and Microsoft do have massive scale and size.

Other benefits of scale include:

- *Multiple Locations*
  Most big cloud providers have the infrastructure and resources to replicate content in multiple locations within their network. This redundancy of content brings some independence from data loss and system failure and also provides a level of disaster recovery
- *Edge Networks*
  The storage, processing and delivery of service closer to network edge means that service quality and reliability would be increased overall and cloud is relatively immune to global network problems.
- *Improved Timeliness of Response*
  Large cloud providers have better resources to detect and mitigate against new malware deployments resulting in more efficient and effective response to cyber threats.
- *Threat Management*
  Cloud providers also have the resources to hire a large and diverse set of cybersecurity specialists, while smaller companies don't have the luxury to afford that.

4.5.2 Security as a Market Differentiator

Since security is a top concern for many cloud customers and as such customer prefer providers who can deliver confidentiality, availability and serviceability. This is a big incentive for cloud providers to be on the leading edge of cybersecurity and deliver best security practices.

4.5.3 Standardized Interfaces for Managed Security Services

Large cloud providers can provide a standardized and open interface to Managed Security Services (MSS) for its customers. This has potential to create a readily available security services market and allows customers to switch providers with relative ease when it comes to security services.

4.5.4 Rapid, Smart Scaling of Resources

Cloud providers have massive amount of resources (e.g. memory, CPU power, storage, virtual machine instances) which they can easily mobilize on demand to counter security threats. A cloud provider has the capability to dynamically allocate resources to increase support for defensive measures (e.g. DDoS attacks) when an attack is likely to happen or already taking place. This offers huge advantages to cloud providers over conventional data centers.

4.5.5 Audit and Evidence Gathering

If an attack happens, a customer can take an image of a live virtual machine for offline forensic analysis, leading to less down time. Multiple clones can also be created and activities can be scheduled in parallel, leading to reduced investigation time and better probability of tracking attackers.

4.5.6 More Timely and Effective Updates

Cloud infrastructure is more likely to be regularly updated with latest anti malware and security patches in a centralized way, making the process more secure and reducing system vulnerability. The virtual machines and software used by customers can also be pre-hardened and updated with latest security patches and security settings.

4.5.7 Audit and SLA's Force Better Risk Management

Security is becoming a key market differentiator among various CSP's and breaches can be detrimental to its reputation. Since more customers are tying in security into Service Level Agreements (SLA), having security breaches can have huge economic consequences for the provider. As such providers are motivated to have rigorous internal audits and risk assessment procedures. The frequent audits imposed on CSP's also help discovering and fixing risks and internal vulnerabilities.

4.5.8 Benefits of Resource Concentration

The concentration of resources has obvious advantages for security. It potentially offers cheaper perimeterization and physical access control and it's easier to implement comprehensive security policy and allows better control over data and patch management, incident response and maintenance processes.

5: Cybersecurity Frameworks and Metrics

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle". Sun Tzu – The Art of War

5.1 NIST Cybersecurity Framework

Cybersecurity threats exploit the vulnerabilities of an increasingly complex and connected systems, including those of the government placing the nation's security, economy and public safety at risk. To better address cybersecurity risk and secure critical technology infrastructure in US, President Barak Obama issued an executive order on Feb 12, 2013:
"It is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" [NIST 2015]. This executive order calls for development of a consensus and collaboration based framework.

The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework [NIST 2014] which can be used by both government and industry. The framework provides a common taxonomy and mechanism for organizations to:

- Describe the current cybersecurity state
- Describe their target or desired cybersecurity state
- Identify and prioritize opportunities for improvement through continuous and repeatable processes
- Evaluate and access progress towards the desired state
- Communicate among internal and external stakeholders about cybersecurity risk

The framework consists of the following three components: (1) Framework Core, (2) Framework Implementation Tiers and (3) Framework Profile. These are discussed in detail below.

5.1.1 Framework Core

The framework core consists of a set of cybersecurity activities, desired outcomes and references that are common across different critical infrastructures. The Core presents industry standards, guidelines and practices in a manner that helps facilitate communication of cybersecurity activities through the length and breadth of the organization from the executive to the operational and implementation level. The framework comprises of five functions –
Identify, Protect, Detect, Respond, Recover. These functions together provide a high level, strategic view of organization's management of cybersecurity risk throughout its lifecycle.

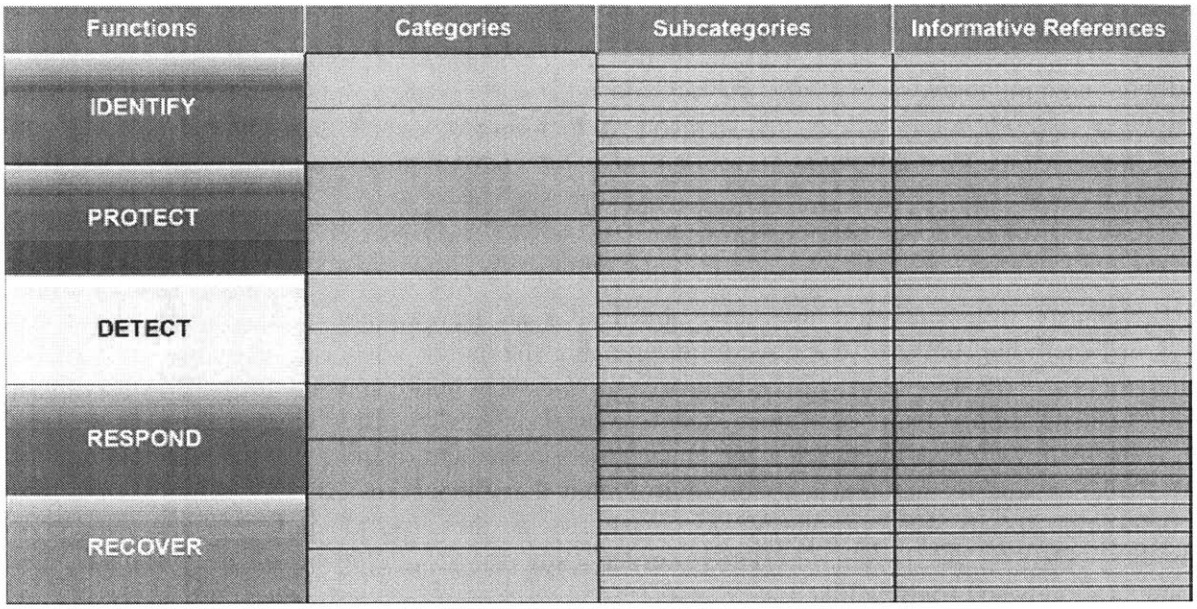


Figure 5.1: NIST Cybersecurity Framework Core Structure [NIST 2014]

The Framework Core elements are described below:

Functions
Functions organize the cybersecurity activities at the highest level. These functions are Identify, Protect, Detect, Respond and Recover. They assist in enabling risk management decisions, addressing threats and improving by learning from previous activities.

Categories
The categories are subdivisions of a function into set of cybersecurity outcomes. Examples of categories include "Asset Management", "Access Control" and "Detection Process".

Subcategories
The subcategories further divide a category into specific technical or management activities and help achieve outcome of the activities.

Informative Reference
These are a set of standards, guidelines and practices that are common across the various critical infrastructure standards.

5.1.2 Framework Implementation Tiers

The implementation tiers provide a context on how the organization views cybersecurity risks and what current processes it has in place to manage these risks. The Tiers describe how mature the organization's cybersecurity risk management practices are, compared to the framework (i.e. risk

and threat aware, repeatable and adaptive). The different Tiers represent the state of maturity of the organization's practices from Partial (Tier 1) to Adaptive (Tier 4).

The Tier definitions are as follows:

Tier 1: Partial
In Tier 1, the organizational cybersecurity risk management practices are not formalized and risk in managed in an unstructured or reactive manner. There is limited emphasis or awareness of cybersecurity risk within the organization. Cybersecurity risk measures are implemented in an ad hoc, case by case basis manner and there is generally lack of processes to promote participation with other entities.

Tier 2: Risk Informed
In this Tier, the risk management practices are approved by management but may not be implemented and practiced in the organization. Although there is awareness of cybersecurity risks at the organization level, processes to manage these risks across the organization have not been established.

Tier 3: Repeatable
In this Tier, the risk management practices are formally approved and written down in policies. These policies are regularly updated based on the business requirements and changing cybersecurity threats. There is also an organization wide emphasis to manage cybersecurity risk. Policies and procedures related to risk and evaluated and updated regularly and the security personnel possess the necessary skills and knowledge to perform their designated roles. The organization also collaborates with other partners and shares and receives cybersecurity related information.

Tier 4: Adaptive
This is the highest tier in this framework and an organization achieves this tier if it has a mature and adaptive cybersecurity practices. It incorporates the lessons learnt and also uses predictive indicators based on its past experience. The organization is in a state of continuous improvement and incorporates advanced cybersecurity technologies and best practices. Cybersecurity is instilled in the company culture and across employees all levels and there is high level of risk awareness of activities on the internal systems and networks. The organization also actively shares information with its partners and ensures that current cybersecurity information is distributed within to improve security before an attack occurs.

5.1.3 Framework Profile

The framework profile can be used to characterize the current "as is" state of cybersecurity with a target profile, desired or "to be" state. Profiles can be used to evaluate the current state of cybersecurity and identify opportunities for improvement and moving to the "target" state. Profiles support business requirements and help in communicating risk both within the organization and with external partners.

5.2 NIST Framework Implementation

Figure 5.2 below describes the flow of information and decisions within a typical organization and comprises of three levels:

Executive
The executive level sets the overall goals and defines the companywide priorities. It allocates resources, and communicates overall risk tolerances to the business/process level.

Business/Process
The business/process level uses the inputs from executive management and develops the risk management process. It also collaborates with the implementation/operations level to communicate the priorities and business needs and creates a risk profile. There is a feedback loop from the business/process level to the executive level to report the overall progress of the risk management process.

Implementation/Operations
Lastly the implementation/operations level provides regular feedback and status updates on the progress of risk profile implementation to the business/operations level.

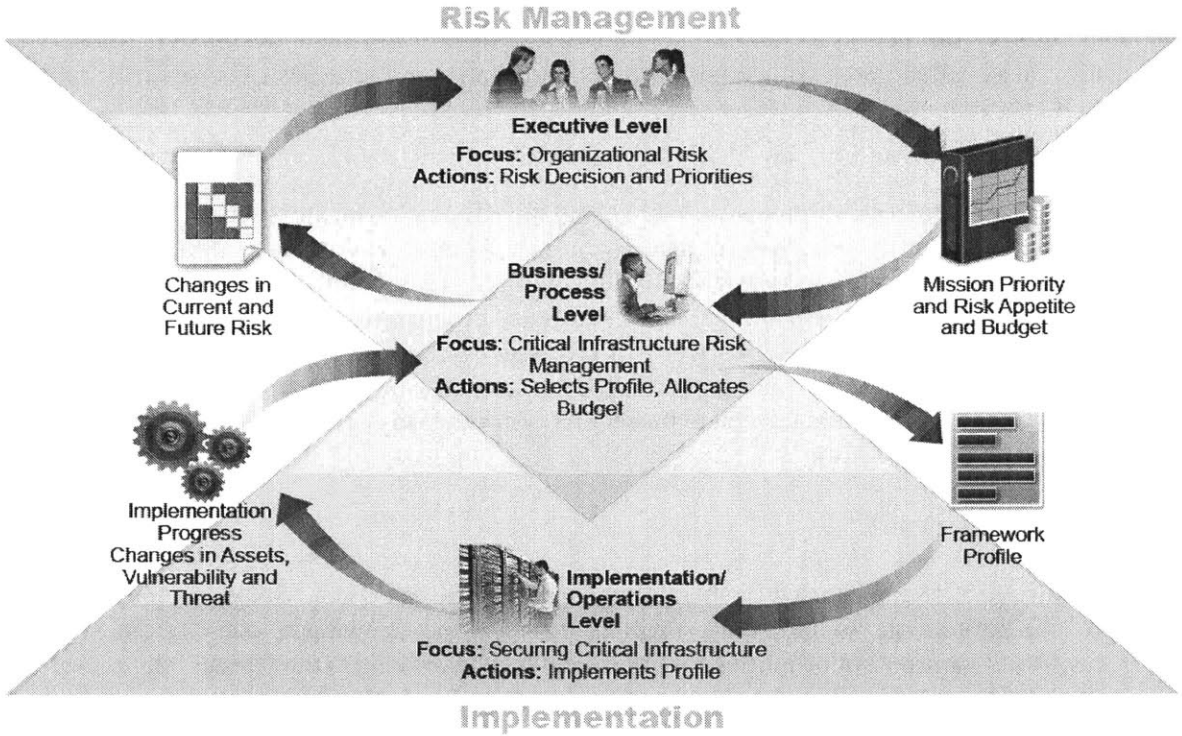


Figure 5.2: Notional Information and Decision Flows within an Organization [NIST 2014]

5.3 CIS Cybersecurity Metrics

To evaluate cybersecurity risks, there has to be way of measuring and quantifying them. One of the key challenges in cybersecurity is having widely accepted and unambiguous metrics for making security related decisions. The Center for Internet Security (CIS) has established a team of over 150 industry experts [CIS 2010] to address this critical need and identified a set of standard metric and data definitions which can be used across organizations for the purpose of measuring and analyzing security related processes. Although each organization has to tailor the metrics based on its individual profile and risk assessment, these metrics provide an important starting point to pursue such decisions.

5.3.1 CIS Metrics Organized by Business Functions

CIS has defined a list of 28 critical security metrics [CIS 2010] which have been broadly classified into different Business Functions such as Incident Management, Patch Management etc. These are described in Table 5.3.1 below.

Business Function		
Function	**Management Perspective**	**Defined Metrics**
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents	Cost of Incidents Mean Cost of Incidents Mean Incident Recovery Cost Mean-Time to Incident Discovery Mean-Time Between Security Incidents Mean-Time to Incident Recovery Number of Incidents
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	Vulnerability Scanning Coverage Percent of Systems with No Known Severe Vulnerabilities Mean-Time to Mitigate Vulnerabilities Number of Known Vulnerability Instances Mean Cost to Mitigate Vulnerabilities
Patch Management	How well are we able to maintain the patch state of our systems?	Patch Policy Compliance Patch Management Coverage Mean-Time to Patch Mean Cost to Patch
Configuration Management	What is the configuration state of systems in the organization?	Percentage of Configuration Compliance Configuration Management Coverage Current Anti-Malware Compliance
Change Management	How do changes to system configurations affect the security of the organization?	Mean-Time to Complete Changes Percent of Changes with Security Reviews Percent of Changes with Security Exceptions
Application Security	Can we rely on the security model of business applications to operate as intended?	Number of Applications Percent of Critical Applications Risk Assessment Coverage Security Testing Coverage
Financial Metrics	What is the level and purpose of spending on information security?	IT Security Spending as % of IT Budget IT Security Budget Allocation
Future Functions	Community recommendations for additional business functions include:	Data / Information Software Development Life-Cycle Configuration Management Third Party Risk Management Additional Financial and Impact Metrics Authentication and Authorization Data and Network Security Remediation Efforts Anti-Malware Controls

Table 5.3.1: CIS Metric Categories Organized by Business Functions [CIS 2010]

5.3.2 CIS Metrics Organized by Hierarchy

These metrics can also be organized based into three different hierarchal levels based on their scope and purpose as defined in Table 5.3.2 below. These are Management Metrics, Operational Metrics and Technical Metrics

Management Metrics:
These metrics provide information about business performance and overall impact on organization.

Operational Metrics:
These metrics are used to understand and optimize the activities of the business functions .

Technical Metrics:
Finally, the technical metrics are used to provide technical details and act as a foundation for other metrics.

As will be seen in the STAMP analysis of Target case later in the thesis, these metrics directly map to the STAMP/CAST hierarchical control structure of Target system.

Metric Categories		
Function	**Management Perspective**	**Defined Metrics**
Management Metrics	Provide information on the performance of business functions, and the impact on the organization. Audience: Business	Mean Cost of Incidents Cost of Incidents Percent of Systems with No Known Severe Vulnerabilities Patch Policy Compliance Percentage of Configuration Compliance Percent of Changes with Security Reviews IT Security Spending as % of IT Budget
Operational Metrics	Used to understand and optimize the activities of business functions. Audience: Security Management	Mean Incident Recovery Cost Mean-Time to Incident Discovery Mean-Time Between Security Incidents Mean-Time to Incident Recovery Mean-Time to Mitigate Vulnerabilities Mean Cost to Mitigate Vulnerabilities Mean Cost to Patch Mean-Time to Patch Mean-Time to Complete Changes Percent of Changes with Security Exceptions IT Security Budget Allocation
Technical Metrics	Provide technical details as well as a foundation for other metrics. Audience: Security Operations	Number of Incidents Vulnerability Scanning Coverage Number of Known Vulnerability Instances Patch Management Coverage Configuration Management Coverage Current Anti-Malware Compliance Number of Applications Percent of Critical Applications Risk Assessment Coverage Security Testing Coverage

Table 5.3.2: CIS Metric Categories Organized by Hierarchical Levels [CIS 2010]

5.4 NIST Cybersecurity Controls

Organizations must have an effective security program in place to identify, control and mitigate security risks to its IT systems. NIST has developed a list of recommended security controls for federal information systems as part of the NIST SP800-53 standard [NIST Metrics]. These controls are listed in Table 5.4 below. For a detailed description on the methodology and description of controls, please refer to the NIST publication [NIST Metrics]. NIST SP800-53 proposes 18 families of security controls organized into 3 classes: Technical, Operational and Management. These security controls are for any generic IT systems and not specifically cloud computing,

therefore they need to be tailored for cloud, based on the individual requirements and security needs of the users and CSP.

NIST SP800-53 Control 18 Families and 3 Classes		
Technical	**Operational**	**Management**
(AC) Access Control (AU) Audit and Accountability (IA) Identification and Authentication (SC) System and Communication Protection	(AT) Awareness and Training (CM) Configuration Management (CP) Contingency Planning (IR) Incident Response (MA) Maintenance (MP) Media Protection (PE) Physical and Environmental Protection (PS) Personnel Security (SI) System and Information	(CA) Certification, Accreditation and Security Assessment (PL) Planning (RA) Risk Assessment (SA) System and Services Acquisition (PM) Program Management

Table 5.4: NIST Recommended Security Controls Organized into 18 Families and 3 Classes [NIST Metrics]

5.5 Cloud Security Alliance (CSA) Cloud Controls Matrix

The Cloud Security Alliance has done extensive work in defining security controls specifically for Cloud services and published Cloud Controls Matrix (CCM) [CSA CCM] to document the different security controls. Its specifically designed to provide security principals to assist CSP's and prospective users in accessing overalls security risk of a cloud provider. The CSA CCM provides a controls framework for the different security concepts and principles that are detailed under the 14 critical security domains discussed in previous chapters. CCM framework is based on and customizes several industries accepted security standards such as ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP [CSA CCM].

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectura		
			Phys	Network	Compute
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X

Figure 5.5: CSA Cloud Controls Matrix [CSA CCM]

6: Service Level Agreements – Cloud

"It is impossible to escape the impression that people commonly use false standards of measurement — that they seek power, success and wealth for themselves and admire them in others, and that they underestimate what is of true value in life."
— Sigmund Freud, Civilization and Its Discontents

To compare the different service offerings, it's essential to have some method of measuring and evaluating service. A user must have clear understanding of the requirements, and create service level agreements (SLA) reflecting these requirements and have a method to measure service in order to validate the delivery and take remedial action in case the service is not as expected. NIST has done some preliminary work in defining metrics for cloud services [NIST SLA]. Metrics can be used at different architectural layers of the cloud computing system (e.g. hardware, platform and services) as well at different stages of the cloud computing life cycle (procurement, operations, retirement). NIST has defined metrics for cloud computing systems at the service interface and classifies these into three general areas: Service Selection, Service Agreement and Service Verification. These are described below.

6.1 Metrics for Cloud Service Selection

Metrics are essential for deciding which cloud service provider to select among the host of options. The user needs to do an internal requirements analysis and then assess the readiness and availability of CSP to meet those requirements. Metrics help to ensure that the CSP has the capability to meet the desired service quality. Figure 6.1 shows the use of metrics to quantify and evaluate the properties of different CSP's before making a decision.

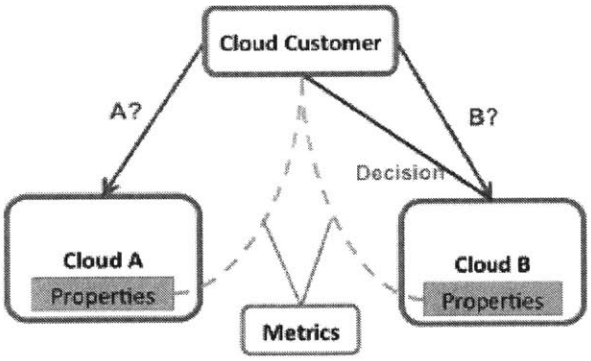


Figure 6.1: Metrics for Cloud Service Selection [NIST SLA]

6.2 Metrics for Cloud Service Agreement

A Service Level Agreement (SLA) is a legal and binding agreement between the CSP and the user. It typically contains the description of the service, the scope of the responsibilities and definition

of the terms of agreement. It can also contain quantifiable and measureable metrics on different aspects of the service. having standardized set of metrics makes it easier to define and converge on SLA's. Figure 6.2 illustrates the use of metrics to define SLA agreements between CSP and user.

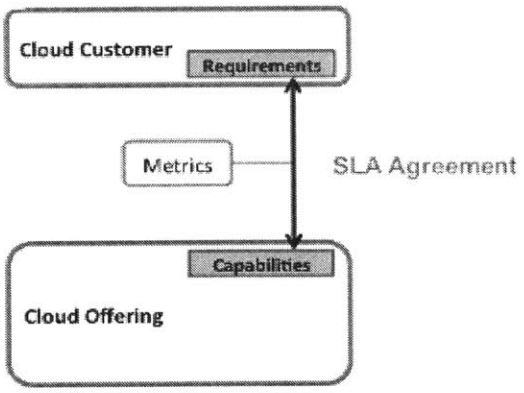


Figure 6.2: Metrics for Cloud SLA Agreement [NIST SLA]

6.3 Metrics for Cloud Service Verification

Once the user purchases the cloud service, it needs to ensure that service level objectives (SLO) are met. Having standard and quantifiable metrics for service during operations helps in ensuring they are met and take remedial action in case they are not. Figure 6.3 illustrates the delivery of service from CSP to user and metrics to monitor the service.

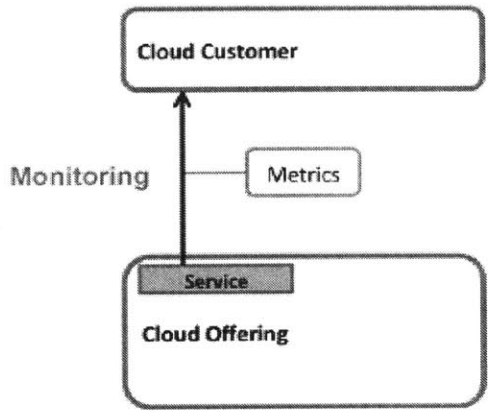


Figure 6.3: Metrics for Cloud Service Verification [NIST SLA]

6.4 Security Metrics for Cloud Service Models

As cloud delivery is beginning to mature, many CSP's offer plausible SLA's for cloud services. While SLA's for ensuring cloud availability have reached a level of maturity, the same cannot be said for SLA's for cloud confidentiality and integrity [SANS SLA]. Implausible SLA's are a major concern for users who want to store and process confidential and sensitive data in the cloud. SANS Institute has proposed set of security controls as part of SLA's for each of the different cloud service models to ensure better cybersecurity in cloud. While these SLA's are not standardized and are in a state of evolution, these offer a framework for starting the discussion on having security controls as part SLA, so that the CSP ensures Confidentiality, Integrity and Availability of user data. The Security SLA's have been mapped to the NIST Security Controls [NIST Metrics] and CSA security controls defined in the Cloud Controls Matrix (CCM) [CSA CCM]. Tables 6.4.1, 6.4.2 and 6.4.3 lists the mapping of SLA's and security controls for IaaS, PaaS and SaaS respectively.

6.4.1 Key Security SLA's for IaaS

The key security SLA's for Infrastructure as a Service (IaaS) are summarized in Table 6.4.1 below.

#	Key Security SLA's Infastructure as a Service (IaaS)	NIST	CSA
1	Change Control and Configuration Management	Configuration Management	Change Control & Configuration Management
2	Data Center Asset Management	Configuration Management	Datacenter Security Asset Management
3	Disaster Recovery and Business Continuity Planning	Contingency Planning	Business Continuity Management & Operational Resilience
4	Secure Configuration and Server Hardening	Configuration Management	Infrastructure & Virtualization Security
5	Malware and Intrusion Prevention	System and Information	Threat and Vulnerability Management
6	Network Vulnerability and Penetration Testing	Risk Assessment	Infrastructure & Virtualization Security
7	Software Lifecycle and Patch Management	System and Services Acquisition	Threat and Vulnerability Management
8	Security Incident Handling	Incident Response	Security Incident Management, E-Discovery & Cloud Forensics
9	Secure Network Protocols and Data Transport	System and Communication Protection	Interoperability & Portability
10	Security Event Logging	Audit and Accountability	Infrastructure & Virtualization Security

Table 6.4.1: Key Security SLA for Infrastructure as a Service (IaaS) [SANS SLA]

6.4.2 Key Security SLA's for PaaS

The key security SLA's for Platform as a Service (PaaS) are summarized in Table 6.4.2 below.

#	Key Security SLA's Platform as a Service (PaaS)	NIST	CSA
1	Change Control and Configuration Management	Configuration Management	Change Control & Configuration Management
2	Secure Application and Program Interfaces	System and Communication Protection	Application & Interface Security
3	Disaster Recovery and Business Continuity Planning	Contingency Planning	Business Continuity Management & Operational Resilience
4	Secure Configuration	Configuration Management	Infrastructure & Virtualization Security
5	Intrusion Prevention	System and Information	Threat and Vulnerability Management
6	Vulnerability and Penetration Testing	Risk Assessment	Infrastructure & Virtualization Security
7	Software Lifecycle and Patch Management	System and Services Acquisition	Threat and Vulnerability Management
8	Data Protection/Portability/Retention/Destruction	Media Protection	Data Security & Information Lifecycle Management
9	Encryption and Key Management	System and Communication Protection	Encryption & Key Management
10	Application and Database Logging	Audit and Accountability	Infrastructure & Virtualization Security

Table 6.4.2: Key Security SLA for Platform as a Service (PaaS) [SANS SLA]

6.4.3 Key Security SLA's for SaaS

The key security SLA's for Software as a Service (SaaS) are summarized in Table 6.4.3 below.

#	Key Security SLA's Software as a Service (SaaS)	NIST	CSA
1	Change and Release Management	Configuration Management	Change Control & Configuration Management
2	Secure Application and Program Interfaces	System and Communication Protection	Application & Interface Security
3	Disaster Recovery and Business Continuity Planning	Contingency Planning	Business Continuity Management & Operational Resilience
4	Secure Configuration	Configuration Management	Infrastructure & Virtualization Security
5	Intrusion Prevention	System and Information	Threat and Vulnerability Management
6	Vulnerability and Penetration Testing	Risk Assessment	Infrastructure & Virtualization Security
7	Software Lifecycle and Patch Management	System and Information	Threat and Vulnerability Management
8	Secure Coding Practices	Awareness and Training	Human Resources Background Screening
9	Identity Access Management	Access Control	Identity & Access Management

Table 6.4.3: Key Security SLA for Software as a Service (SaaS) [SANS SLA]

6.4.4 Summary of Key Security SLA for the Three Cloud Services

Table 6.4.4 below provides a summary of security SLA's for the three different types of delivery models, for a quick comparison.

#	Key Security SLA's Cloud	NIST	CSA	IaaS	PaaS	SaaS
1	Change Control and Configuration Management	Configuration Management	Change Control & Configuration Management	Yes	Yes	Yes
2	Data Center Asset Management	Configuration Management	Datacenter Security Asset Management	Yes	No	No
3	Disaster Recovery and Business Continuity Planning	Contingency Planning	Business Continuity Management & Operational Resilience	Yes	Yes	Yes
4	Secure Configuration and Server Hardening	Configuration Management	Infrastructure & Virtualization Security	Yes	Yes	Yes
5	Malware and Intrusion Prevention	System and Information	Threat and Vulnerability Management	Yes	Yes	Yes
6	Network Vulnerability and Penetration Testing	Risk Assessment	Infrastructure & Virtualization Security	Yes	Yes	Yes
7	Software Lifecycle and Patch Management	System and Services Acquisition	Threat and Vulnerability Management	Yes	Yes	Yes
8	Security Incident Handling	Incident Response	Security Incident Management, E-Discovery & Cloud Forensics	Yes	No	No
9	Secure Network Protocols and Data Transport	System and Communication Protection	Interoperability & Portability	Yes	No	No
15	Security Event Logging	Audit and Accountability	Infrastructure & Virtualization Security	Yes	No	No
10	Secure Application and Program Interfaces	Audit and Accountability	Infrastructure & Virtualization Security	No	Yes	Yes
11	Data Protection/Portability/Retention/Destruction	Audit and Accountability	Infrastructure & Virtualization Security	No	Yes	No
12	Encryption and Key Management	Audit and Accountability	Infrastructure & Virtualization Security	No	Yes	No
13	Secure Coding Practices	Audit and Accountability	Infrastructure & Virtualization Security	No	No	Yes
14	Identity Access Management	Audit and Accountability	Infrastructure & Virtualization Security	No	No	Yes

Table 6.4.4: Key Security SLA for IaaS, PaaS and SaaS

7: Cloud Migration Strategy and Framework

"A life spent making mistakes is not only more honorable but more useful than a life spent doing nothing." George Bernard Shaw

Deciding whether, what, when and how to move to cloud is something which almost every organization has to face and it's quite a complex decision with many variables at play. Companies have to evaluate the associated risks, especially security with benefits and ROI. Cloud organizations such as CSA and international network and security agencies such as ENISA [ENISA 2009] have developed recommendations and risk scenarios for the different kinds of cloud deployments and services. Ultimately the needs and requirements of each organization are different as well as the associated risk profile. While it's very difficult to come up with a set of frameworks which is applicable to the entire spectrum of industries and businesses, this research presents a generalized high level framework which can act as a starting point to help start the discussion about cloud migration and evaluating the risks and benefits of the same. This framework is adapted from the framework described in CSA Report on Security Guidance for Critical Areas of Focus in Cloud Computing [CSA 2009]. Inputs from McKinsey research reports [McKinsey 2011] and Amazon Web Services (AWS) have also been taken [AWS 2010]. This research builds upon the previous recommendations and also integrates systems engineering tools and methodologies to help support the complex requirements gathering, risk evaluation and ultimately multivariate decision making.

7.1 Migration Framework Flowchart

Figure 7.1.1 below, describes the high level framework for cloud migration and is discussed below.

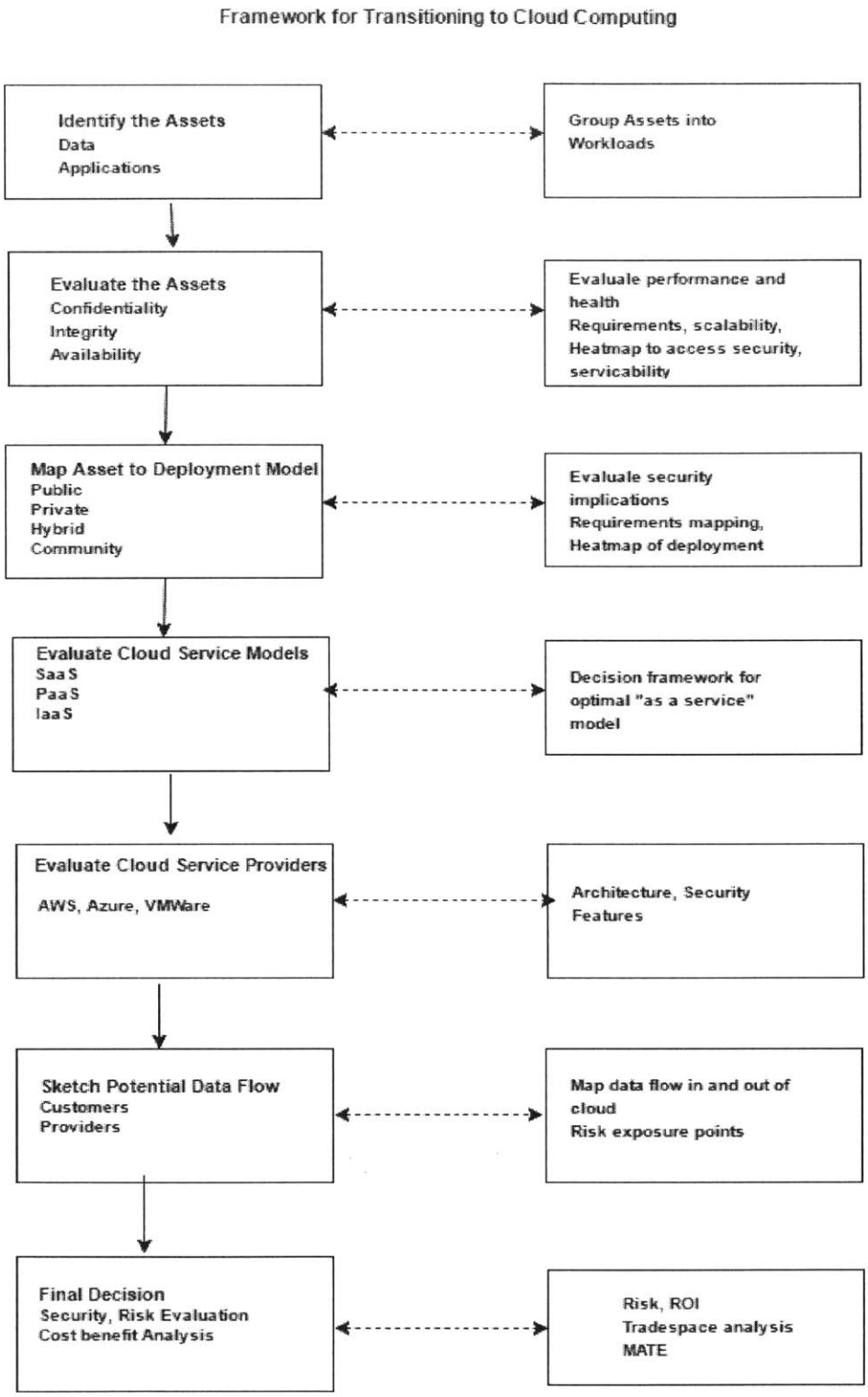


Figure 7.1.1: Framework for Transitioning to Cloud

7.1.1 Step One: Identify the Assets for Cloud Deployment

The first step is to identify the assets within the company which can be suitable for cloud deployment. Broadly assets fall into two categories, data and applications. Either data or information can be moved into cloud or we can also migrate full software applications. The assets can be migrated only partially and moved to several different cloud locations. One major factor to consider is exactly what kinds of data or functionality to migrate and evaluating associated risks. An organization can have hundreds of data sets and potentially thousands of applications. According to recommendations by McKinsey, applications should be bucketed into 30-50 workloads which have similar applications. For e.g. instant messaging, email service, calendaring can all fall under collaboration and messaging workload. The workload should be broad enough that a commercially available software package can deliver but should not too be broad as otherwise it will not be a useful basis for analysis.

7.1.2 Step Two: Evaluate the Assets for Cloud Deployment

Once the assets have been identified, the subsequent step is to evaluate how critical or sensitive the asset is to the organization. To facilitate such evaluation, below is a set of some questions that need to be asked [CSA 2009].

- What would be the impact if the asset becomes widely and publicly distributed?
- What would be the impact if an employee of cloud provider accessed the asset?
- What would be the impact if the asset is manipulated by a malicious outsider?
- What would be the impact if the asset fails to provide expected results in the cloud?
- What would be the impact if the information/data were unexpectedly changed?
- What would be the impact if the asset becomes unavailable for a period of time?

We need to evaluate Confidentiality, Integrity and Availability (CIA) requirements for the asset. In essence these are similar to any conventional IT data center, but with added security dimension of being moved to cloud and hence being outside the physical perimeter of the company. To add to that, there are a variety of cloud deployment vendors, deployment models and types of delivery service.

The organization needs to evaluate the health and performance for each workload identified in the above step which essentially means the degree to which the current solution meets current and future needs of the company. Criteria which can be used include end user satisfaction, ease and affordability to make changes for new requirements and ease of scaling to address spikes in demand. Typically, candidates which are low scoring on performance and have less stringent security requirements are ideal candidates for cloud. Figure 7.1.2 below provides a simple framework to access the security and manageability of workloads. The heat map below rates all the different workloads (e.g. human resources, engineering development) against the different company requirements in security and manageability domain. The requirements vary for each workload and the green ones better suited for cloud migration than the red ones.

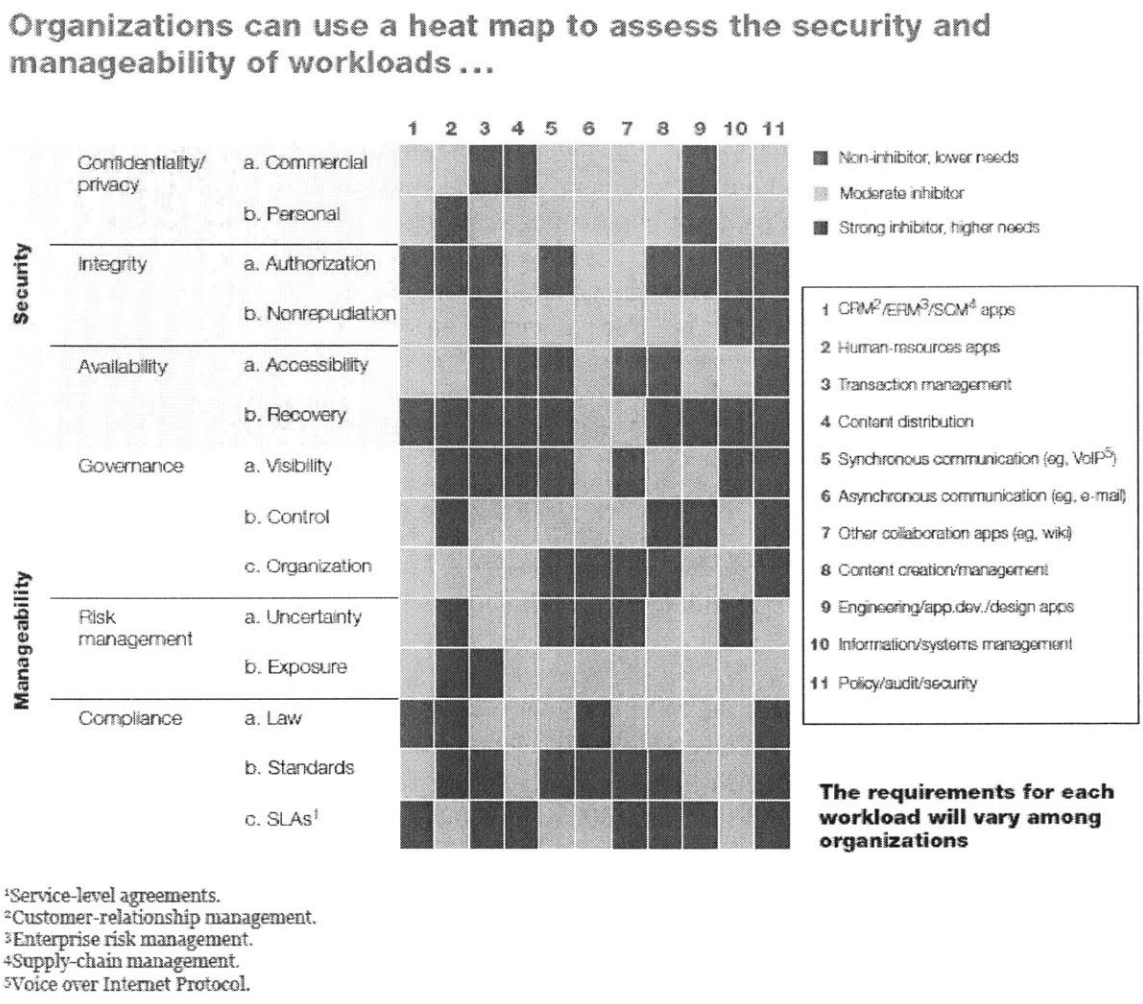
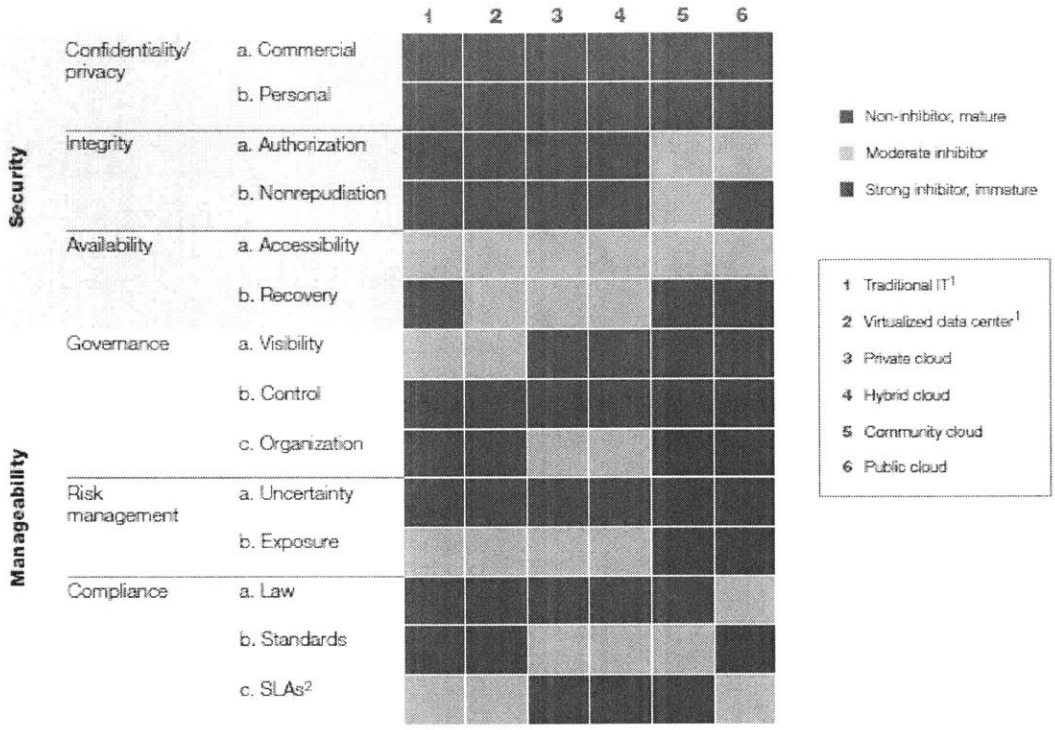


Figure 7.1.2: Heat map to Access Serviceability and Manageability of Workloads [McKinsey 2011]

7.1.3 Step Three: Map the Asset to Potential Deployment Models

After the assets are evaluated and ranked, the next step is to determine which cloud deployment model is suitable for migration. The broad definitions as well as the risks and benefits have already been discussed in the previous sections. The main kinds of deployment models include public cloud, private cloud (internal/external deployment), hybrid cloud and community cloud.

The security risks associated with each architecture should be carefully understood and evaluated against the risk tolerance of the asset. To assist in this process, tools such as heat map and Quality Function Deployment (QFD) can be used. Figure 7.1.3 below, illustrates the heat map of the security and manageability of deployment models. The requirements can be decomposed further depending on the specific security requirement and importance of the assets.

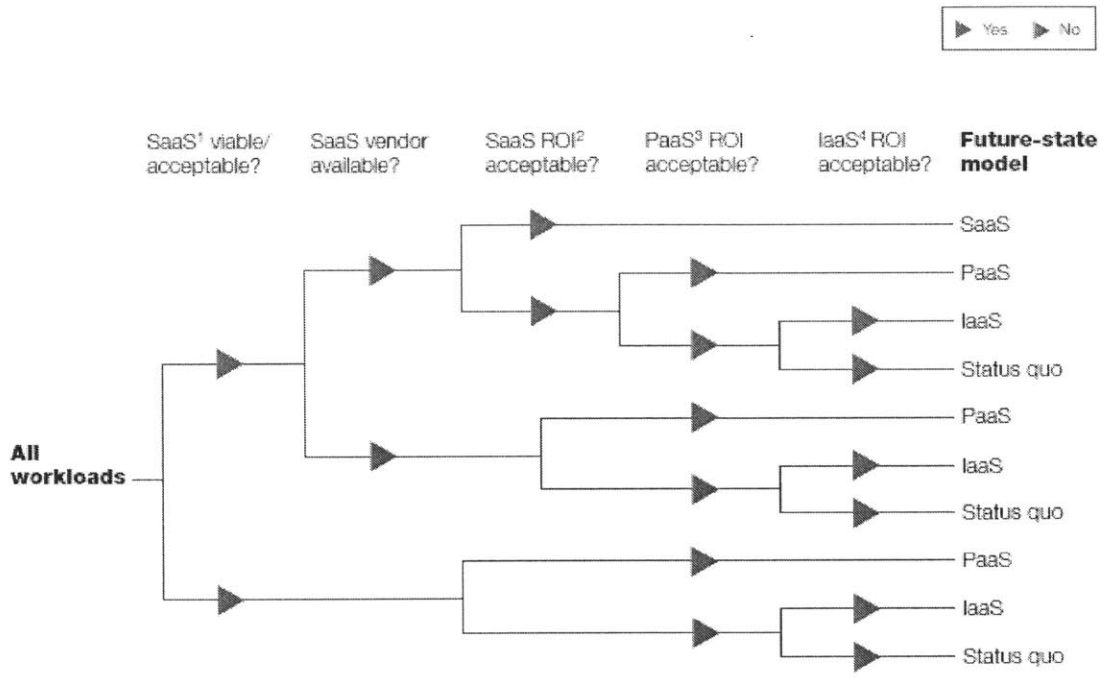


[1]Could be either on- or off-premises, captive, or outsourced.
[2]Service-level agreements.

Figure 7.1.3: Heat map to Access Serviceability and Manageability of Deployment Models [McKinsey 2011]

7.1.4 Step Four: Evaluate Potential Cloud Service Models

In this step the focus is to map the assets to the various service models (SaaS, PaaS, IaaS). The degree of control and risk profile is different for the different tiers and has been discussed in previous sections. Depending on the kind of workload or specific workload requirements (ROI, portability, security) an organization has to make a decision among the various service deployment models (SaaS, PaaS or IaaS). For example, an organization which prioritizes speed of implementation and deployment over control and customization may prefer SaaS over PaaS and IaaS. The decision tree for a company which prefers SaaS is given in the Figure 7.1.4 below. In this decision tree, the company first favors SaaS and evaluates the ROI and risks associated with this service. If it's not acceptable, then evaluates the PaaS delivery model followed by IaaS. In some cases, there is no clear yes or no answer and instead there's a status quo.



[1]Software as a service.
[2]Return on investment.
[3]Platform as a service.
[4]Infrastructure as a service.

Figure 7.1.4: Decision Framework to Choose Optimal "as a service" Model [McKinsey 2011]

7.1.5 Step Five: Evaluate Potential Cloud Service Providers

After doing a preliminary risk evaluation, the next step is to switch to a full security risk evaluation based on the specific architectural details and security offerings of the cloud vendor for e.g. AWS, Azure, VMware etc. Each of these CSP's have a different architectural implementation of cloud and offer different security features and security controls. They also have varying degrees of readiness and willingness to list the security expectations in SLA's. Companies which have more confidence in their security infrastructure will be more willing to guarantee security features. The company needs to evaluate all these options and decide which of these providers' best fits its security needs. Big companies also provide Total Cost of Ownership (TCO) tools which also helps in accessing the economic feasibility of the decision. Table 7.1 below describes a high level comparison of the costs of maintaining a typical IT data center versus a cloud offering.

Pricing Model	One-time Upfront Cost		Monthly Cost	
	CSP	Traditional	CSP	Traditional
Server Hardware	-	$	$	-
Network Hardware	-	$	-	-
Hardware Maintenance	-	$	-	$
Software OS	-	$	$	-
Power and Cooling	-	$	-	$
Data Center	-	$	-	-
Admin	-	$	$	$
Storage	-	$	$	-
Bandwidth	-	$	$	$
Resource Management Software	-	-	$	$
24x7 Support	-	-	$	$

Table 7.1: Comparison of Pricing Models of Traditional Data Center versus Cloud [AWS 2010]

As is illustrated in Table 7.1, there are significant one time upfront costs while setting up a traditional data center versus a cloud. It also takes time to setup the data center to get it functional while cloud has a much shorter startup time. The downside is that in a typical cloud offering, the monthly costs are higher as compared to costs of a traditional datacenter. While doing the TCO calculation, specifically the security costs also need to be compared as security can represent a big proportion of the typical data center cost depending on how critical the application and data is.

In a typical data center, the security expenses are mainly related to the following

- Software: Firewall, Antivirus, Malware
- IT Security Staff
- Certification and accreditation
- Auditing and monitoring

Some of the Metrics that can be used to analyze security and costs associated with it include [CIS 2010]

- IT Security Spending as % of IT Budget
- IT Security Budget Allocation,
- Risk Assessment Coverage

In cloud, security costs need to be factored in as well. The security control and costs vary with the service model. Some of the security costs are listed below [TechTarget Cloud]. However, user still needs to take care of certain security costs. Even for SaaS, the customer needs to have some implementation of Identity Access Management (IAM)

Security Costs Cloud:

- Service Model – IaaS, PaaS, SaaS

The degree of control for the user decreases as one moves from IaaS to PaaS to SaaS. According security costs should typically decrease as CSP takes greater ownership of security features.

- Cloud Security Engineers [TechTarget Cloud]
  Cloud security engineers are in high demand, represent a scarce resource and command high salaries.
- Cyber Insurance (Higher Premium?)
  The cyber insurance rates could potentially go up as cloud services have generally higher degree of risk associated with them.
- Identity Access Management (IAM)
  IAM needs to be implemented for SaaS applications on cloud. While certain CSP's provide it as part of the package, some don't.

All these costs have to be factored in before making the decision.

7.1.6 Step Six: Sketch the Potential Data Flow

After evaluating the specific deployment model and vendor, it's essential to map out the potential data flow from the cloud to the customers and understand how the data moves in and out of the cloud. One has to analyze the risk exposure points and the likely consequences in case of a security breach. One must look at possible ways to mitigate risk exposure before making the final go-no-go decision.

7.1.7 Step Seven: Making the Final Decision

At this stage, one should have an understanding of the important factors to consider for moving to the cloud, the risk tolerance as well as the various combinations of deployment model and service offerings which seem acceptable. One also has an idea about the potential exposure points for sensitive information leaks and security hazards. If the company decides to seriously consider moving some workloads to cloud, it must perform a comprehensive security and risk evaluation as well as cost benefit analysis before making the final recommendation. Since this decision is extremely complex with several variables operating across different dimensions, a comprehensive exploration of the trade space is required. The Multi-Attribute Tradespace Exploration (MATE) methodology which was developed at MIT for exploring tradespaces of possible architectures rather than settling quickly on an optimum is one such powerful method to arrive at the optimal decision [MIT MATE, Ross 2005]. MATE is a structured program selection process and selects a decision which is right for the organization's stakeholder needs and is widely used in arriving at complex decisions for complex engineering problems over its complete lifecycle. MATE may be used in conjunction with other decision making techniques and risk evaluation frameworks used by the company. While making the decisions, the well-known cybersecurity frameworks such as those developed by NIST as well as specific to cloud security such as CSA guidelines and ENISA recommendations should be used as a reference.

7.2 Migrating to Cloud – Target Case as an Example

To better reinforce the cloud migration framework and apply the security concepts discussed so far, we can apply this framework to a real company which has been the victim of cybersecurity breach and try to answer the question whether its threat profile would have reduced had it tapped into some of the security benefits that CSP's offer and migrated some of its less critical applications to cloud. We can also get the opportunity to apply the security frameworks, security controls as well as some oft security metrics discussed previously and understand if these were not properly applied by the company or not monitored accurately. We need to do a root cause analysis of the cybersecurity accident and identify main causal factors which led to security breach in the first place. For the purpose of this analysis, we shall use the Target data breach as an example [Target 2014]. The attack happened in Dec 2013 and was one of the largest data breaches in US history at that time. We shall apply STAMP framework to analyze the accident and identify key list of recommendations based on our analysis. During the process, we will also identify security controls that were missing that could have helped in tracking security compliance. We will finally attempt to apply the cloud migration framework to Target case and answer the question, whether migrating to cloud could have alleviated some of the security risks that Target was exposed to.

8: Target Attack Overview

"Success breeds complacency. Complacency breeds failure. Only the paranoid survive." - Andy Grove, Former Intel CEO

On 19th Dec 2013, US based retail giant Target released a statement that it had been victim of a major cyber-attack and a security breach. The credit card data of about 40 million Target customers was stolen between Nov 27th and Dec 15th. This press release came a day after it was first reported by Brian Krebs, an independent internet security news and investigative reporter on Dec 18th.

It was the Department of Justice (DOJ) that first informed Target on 12th Dec, about the occurrence of this cyber-attack. From the various research reports on the breach, it seems Target was not aware of any attack or wrong doings inside its systems, till it was alerted by DOJ and they also testified in US Congress about lack of awareness of this attack [Kill Chain 2014]. Target sought the help of federal law agencies, including the Secret Service and DOJ to investigate this incident. On 23rd Dec, Target suggested that a malware installed on point of sale (POS) terminals was a key component of the breach. This was later confirmed by Target in Jan 2014. Target however did not release much of the technical details on the attacks. Research teams such as Dell SecureWorks Counter Threat Unit (CTU) [Dell 2014] did independent analysis on this incident to throw some light into the technical details of the attacks. There was also a report submitted to the United States Senate Committee on Commerce, Science and Transportation which did in-depth analysis of the Target cyber-attack [Kill Chain 2014].

Thieves were able to sell information from cards via online black market forms called "card shops". These websites listed credit card information such as card type, expiration date, track data (account information which is stored on the credit card's magnetic stripe), issuing bank and successful rate for card batches over time [Kill Chain 2014]. The newer batches were priced higher than older batches, since issuing banks would not have enough time to disable and cancel the compromised cards. On Jan 10th, 2014 Target disclosed that personal non-financial information of about 70 million customers [Elgin 2014], including names, addresses, phone numbers and email addresses were also stolen during this data breach [Target 2014].
Public records, however do not indicate how the attackers got access to this data. Thus a total of about 110 million Target customers had their personal data compromised in this massive data breach [Zdnet 2015].

8.1 Analysis of the Attack

The original point of entry into Target's internal network is unknown. Similarly details about attacker's tactics, techniques and procedures (TTP's) after they gained initial access to the network is also not known. However, research teams were able to find out the following technical details about the attack after completing their analysis. [Kill Chain 2014, Zdnet 2015, Dell 2014, SANS 2014]

- The attackers may have carried out initial reconnaissance using a Google search. This would have supplied lot of information about how Target interacts with its vendors, while also providing a vendor portal with list of HVAC and refrigeration companies. Along with that, the reconnaissance most likely would also have revealed detailed case study on Microsoft website that described how Target used its virtualization software, centralized name resolution as well as Microsoft System Center Configuration Manager (SCCM) and information about how Target deploys its security patches and updates. It also described in great detail, Target's POS system.
- An email containing the malware was sent to the refrigeration HVAC vendor, Fazio, two months before the credit card breach. Malware installed on Fazio's machine might have been Citadel, which is a password stealing program, a derivative of Zeus banking Trojan. This malware stole credentials to Target's online vendor portal thus providing a foot hold into its system [Krebs 2014].
- After getting the credentials, the attackers accessed Target's systems via Fazio's vendor portal.
- From this point onwards, the attackers could have done further reconnaissance on Target's internal network to look for vulnerabilities and move laterally within Target's system via backdoors and other system vulnerabilities.
- Another report on Target's data breach describes how reconnaissance in Target's attack revealed several misconfigured systems. A vulnerable domain controller could have been used to obtain access to POS systems. [Mandiant 2014]
- Microsoft's case study on Target attack also reveals that each retail store functioned as an autonomous unit except for centralized authentication, domain name resolution and end point monitoring services. (Microsoft 2011). The attackers might have focused on these pivot points.
- After gaining access to the vulnerable systems, the attackers would have moved to install malware on Point of Sale systems (POS).
- After gaining access to the vulnerable systems, malware was installed on the Point of Sale Systems. Also since a large number of terminals were affected, it appears that the malware was installed using an automated process. The Dell SecureWorks report indicates that the malware was likely installed using System Center Configuration Manager (SCCM) [Dell 2014].
- The malware used "RAM scraping" attack, which allowed for the collection of unencrypted, credit card and personal info of the customers, as the cards were swiped at the terminals. This data was stored in a .dll file. [iSight 2014]
- This data would be periodically moved off the system using customized components. Reports also indicate that data was retrieved using default user name and password for BMC's performance assurance for Microsoft Servers.
- Data was moved to drop locations on hacked servers to many parts of the world using File Transfer Protocol (FTP). The attackers retrieved this data from drop locations.
- Target's monitoring software (FireEye) sent alert notifications (malware.binary) to its staff in Bangalore, India. They in turn notified the Target IT staff in Minneapolis, however no action was taken. [Elgin 2014]. The system had the option to delete malware automatically as it was detected, however this option had been turned off. So there were shortcomings at multiple levels.

- The hackers extracted credit card and personal information from the raw data and sold it on the black market. [Krebs 2013]

8.2 Malwares Used

As per the reports of the investigation, the attackers used two different malware families within Target's network. The first malware stole raw payment card data from the memory and was installed on the POS terminals. This malware used "RAM scraping" attack, which allowed for the collection of unencrypted, plain text data as it was transferred from the company's POS machine memory before being transferred to the company's payment processing center. Over 11 GB of consumer data was stolen. According to reports by Brian Krebs [Krebs 2013], this malware was available on the black market for between $1800 to $2300 and was installed on Target's POS. McAfee's Director of Threat Intelligence Operations described this malware as "absolutely unsophisticated and uninteresting" [Elgin 2014].

The second malware transmitted stolen data outside the network to certain data drop locations. This malware thread would awake an hour after its launched and would attempt to exfiltrate credit card data between 10am to 6pm, usually the time of high activity in the store to mask its activity. A third type of malware was also known to exist on intermediate dump servers inside Target's network but no samples were identified. Figure 8.2 [Dell 2014] below describes the flow of data exfiltration from Target's internal networks and the location of malware installed.

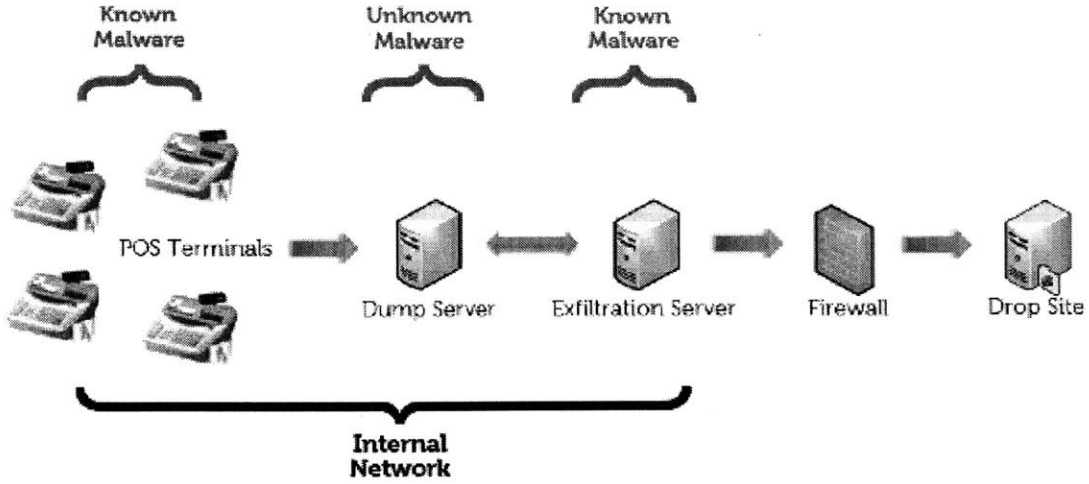


Figure 8.2: Target Data Exfiltration Malware [Dell 2014]

The details of the first two type of malwares are given below.

POSWDS

On Dec 20th, 2013 the US Department of Homeland Security, National Security and Communications Integration Center (DHS NCCIC) in collaboration with US-CERT, released Malware Findings Report, which detailed a malware sample which was designed to target a POS system and facilitate payment of raw credit card data. This malware installs as a system service,

ensuring that it automatically starts on system reboot and is persistent. The malware image name (svchosts.exe) is identical to Windows Service host process(svchost.exe), ensuring that its effectively blended in the compromised system. The executable files' location and its ability to install as a service shows that the Administrator's account on the affected POS systems had been compromised.

The second malware would exfiltrate data by creating a mount point for a remote file share and copy data stored by memory scrapping component onto that file share. The malware code would read the process's memory space in 10 MB chunks. The memory would be processed by a heuristic algorithm attempting to track credit card data. Card data would be written into a winxml.dll file and periodically moved off the system.

The hackers used additional component on the host apart from POSWDS, to migrate stolen data from Target's internal network. through the firewall to a drop site outside their network. The Dell Counter Threat Unit (CTU) team identified as many as five variations of this malware.

BlackPOS

After the technical details of the Target breach emerged, the malware has been associated with the BlackPOS malware created by a user "ree4". The author called the malware, "Dump Memory Grabber" and sold it on criminal forums in early 2013 for an asking price of 2000 Liberty Reserve (LR). Earlier versions of the BlackPOS had been known to be circulating since early 2010. CTU researchers believe that the most likely scenario was that the Target attackers used the original memory monitor source code as a foundation for their custom malware.

8.3 Aftermath and Repercussions of Attack to Target

This cyber-attack had serious repercussions to Target customers, management as well as issuing banks. Personal data of about 110 million Target customers was stolen or compromised. Several top employees including the CEO [Gonsalves 2014] and CIO [Baldwin 2014] lost their jobs. Target's board of directors were also threatened with removal. The issuing banks of Target's credit card also suffered enormous monetary consequences. They had to refund stolen money from Target's customers via credit card and it cost them over $200 million. There were also several law suits filed against Target. Banks also filed a lawsuit against Trustwave, Target's PCI compliance auditor. The Department of Justice, Federal Trade Commission and SEC also started investigations against Target. All this resulted loss of reputation and trust of Target and with the result its sales and profits dropped, resulting in further economic loss. According to Target's quarterly report (Feb 25th 2015) the total breach expenses incurred amounted to $162 million (total 2013 and 2014 expenses). Full-year net breach expenses for 2014 were $145 million ($191 million offset by $46 million insurance receivable). There are several public reports available which analyzed the full spectrum of economic losses suffered by various stakeholders linked to Target due to the data breach. The findings of these reports are summarized in the Table 8.3 below.

Loss Estimates			
Total per Incident	**Per Card**	**Source**	**Comments**
$4.9 billion	$122	Ponemon (2013)	Estimate based on 40 million cards at general retail cost of $122/card
$1.4-$2.2 billion fraud	$35-$55 fraud	Jefferies (2014)	Target, limited costs considered
$400 million-$1.1 billion PCI fines	$10-$28 PCI fines		40 million cards
$240-$600 million	$6-$10	Visa/Jefferies (2014)	Replace fraud rates used by Jefferies with Visa's fraud rates
			40 million cards
$61 million gross	$1.10	Target (2013)	Reported for fourth quarter 2013 only
$17 million after insurance	$0.28		40 million cards
$11 million after insurance and taxes			Total costs not yet known

Table 8.3: Target- Summary of Loss Estimates for Target Credit Card Data Breach [Weiss 2015]

8.4 PCI-DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card companies. The PCI Standard [PCI] is mandated by the credit card brands and administered by the Payment Card Industry Security Standards Council. This standard was created to increase safety around cardholder data to reduce credit card fraud.

Following the PCI standards and being compliant is a necessary but not sufficient condition, as the Target breach shows. PCI compliance only focused on the credit card payment processing. As such it has a very narrow focus and many businesses try to minimize its scope, so as to pass the PCI audit. According to many critics of PCI audits, "the PCI system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties" [Mccombs].

There are several systems and assets which fell outside the scope of PCI audits and hence they may pose greater risk, if organizations solely focus on PCI audit. For e.g., at the time of Target security breach, the PCI security standard specification mentioned that consideration should be

made for credit card data stored in computer memory, however no specific requirements were defined as to how data should be secured.

Also hackers have the same access to PCI standards and security measures as corporations and they are constantly looking for vulnerabilities and develop tactics to exploit such weak points. Developing and implementing regulations and standards takes time. As such companies have to be one step ahead and continuously look for weaknesses within their system that the attackers might exploit. So just having a mandated checklist for PCI is clearly not enough and organizations need to perform companywide risk assessment and management activities. Threats and vulnerabilities for all systems, not just those which fall under compliance audit, should be identified.

Target had passed PCI compliance audits prior to the breach, indicating that they had passed the security requirements required by the credit card processing industry. Target's HVAC vendor, Fazio also passed a statement that they had followed the required security measures and were in compliance with industry standards.

8.5 Opportunities Missed by Target

Target missed a number of opportunities to stop the attackers and prevent this massive data breach. According to the publicly available reports, some of the key points which Target failed to detect and prevent this attack, include the following list below [Elgin 2014, Aorato 2014]. This list is by no means complete as it's just based on what is available publicly.

Target gave network access to a third party vendor, a small Sharpsburg Pennsylvania based HVAC and refrigeration company, Fazio Mechanical Services. This company specialized in refrigeration contractor for big supermarkets in the mid-Atlantic region. It had remote access to Target's network for electronic billing, contract submission and project management purposes. This company did not follow the accepted security practices and as a result its weak security profile left a door open for the attackers to gain a foothold in Target's network.

The attackers first gained access to Target's system by stealing credentials from the HVAC company from emails infected with malware. According to target's security team, Fazio most likely had access to Target's Ariba billing system. However, it's not clear how the attackers managed to gain access to Target's POS terminals from the initial foothold on the periphery of its network. According to its security team, it's very likely that the outside portal was not fully isolated from the rest of Target's network. Once the attackers gained a foothold, they might have hacked a default account name used by IT management software product by BMC Software, to gain access to Target's internal network. The attackers also disguised their data exfiltration malware as an authentic BMC Software product,

Target's anti-intrusion software had issued multiple security warnings about a malware being installed by the system, however it appears that the company failed to recognize that or take any measures to investigate the situation. Target's Symantec antivirus software detected malicious behavior around November 28th 2013, however the company failed to take any actions.

Once the attackers gained foothold into Target's network, they moved from the less sensitive areas of the network to more sensitive areas where consumer data and credit card information were stored. This suggests that Target was unable to partition and isolate their more sensitive network assists or have additional security measures in place for these high value areas.

Target also failed to respond to multiple warnings issued by the company's anti-intrusion software which indicated that the attackers were planning to exfiltrate data from its network and also provided details of the escape routes. According to Bloomberg Businessweek report, Target's FireEye malware intrusion detection system, trigged urgent alerts about the installation of data exfiltration malware. Target's security team in Bangalore, India did receive the alert and notified Target's IT team in Minneapolis. However, Target's security team did not respond and nothing happened. FireEye software also had the option to automatically delete the malware, however this feature had been disabled [Elgin 2014].

All this suggests that just following minimum security measures and following baseline standards in not enough and a holistic approach to cybersecurity is required. Each asset must be analyzed in relation to its place in the overall system and all vulnerabilities must be guarded with countermeasures. The attackers will always find and exploit the weakest link in the security chain. A Systems Approach to cybersecurity which targets not just technologies but also the role of humans and their interaction with the systems, can help both analyzing the root cause of attacks and systemic problems as well as also mitigate some of the weak points that attackers use to exploit the system.

9: Systems Thinking Approach to Managing Cybersecurity Risks - STAMP Framework Overview

"He shall divide both the day and the night into eight nalikas [1.5 hours]. Of these divisions, during the first one-eighth part of the day, he shall post watchmen. during the fifth, he shall receive the secret information gathered by his spies; During the first one-eighth part of the night, he shall receive secret emissaries; during the seventh, he shall sit considering administrative measures and send out spies; Or in conformity to his capacity, he may alter the time-table and attend to his duties." Book I, Chapter 19, The Duties of a King – Chanakya's Arthashastra

In traditional causality models, accidents are supposed to be caused by a chain failure events. This definition of accidents is no longer adequate for today's complex socio technical systems. Accidents must include not just the failure events but also component interactions, direct or indirect as well as systemic causal failures, leading to the accident. In Systems Theory, safety is an emergent property which arises from the interactions among system components. The Systems-Theoretic Accident Model and Processes (STAMP) framework is a causation model and accident analysis method based on systems thinking that can be used to improve the design, operation, and management of systems.

9.1 STAMP Core Concepts

The STAMP model has the following Core concepts [Leveson 2011]

- Safety Constraints
- Hierarchical Safety Control Structures
- Process Model

9.1.1 Safety Constraints

In STAMP framework, the most basic concept is not an event but a constraint. Events lead to losses only because safety constraints were not successfully enforced. So STAMP emphasizes not in preventing failure events, but in modelling effective controls for enforcing constraints, which prevent such failures.

9.1.2 Hierarchical Safety Control Structures

In Systems Theory, systems are viewed as hierarchical structures, in which each level imposes constraints on the level below it. Therefore, the higher level controls the actions and behaviors of the level below it, by using constraints. Control processes operate between levels to control processes at the lower level in the hierarchy, governed by a standard feedback loop structure depicted in Figure 9.1.1. Accidents occur when these processes provide inadequate control and safety constraints are violated in the behavior of lower level components.

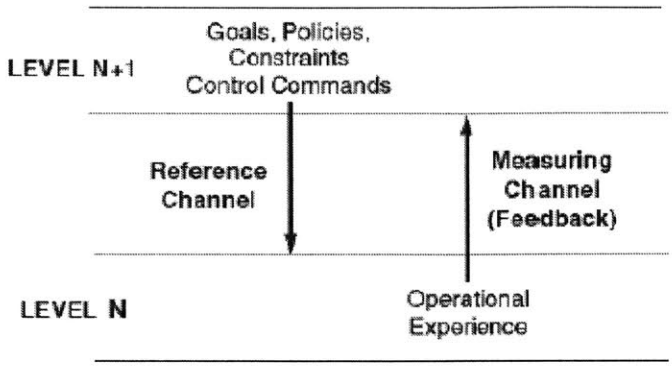


Figure 9.1.1: Communication Channels between Control Levels [Leveson 2011]

At each level in this hierarchical structure, inadequate control may result from the following

- Missing constraints or unassigned responsibility for safety
- Inadequate safety control commands
- Commands that were not executed correctly at lower level
- Inadequately communicated or processed feedback about constraint enforcement

Effective communication is needed between the hierarchical levels of the safety control structure, including both a downward reference channel providing necessary instructions to impose safety constraints on the level below as well as an upward measuring channel to provide feedback about how effectively the constraints are being satisfied. Figure 9.1.2 describes the standard control loop.

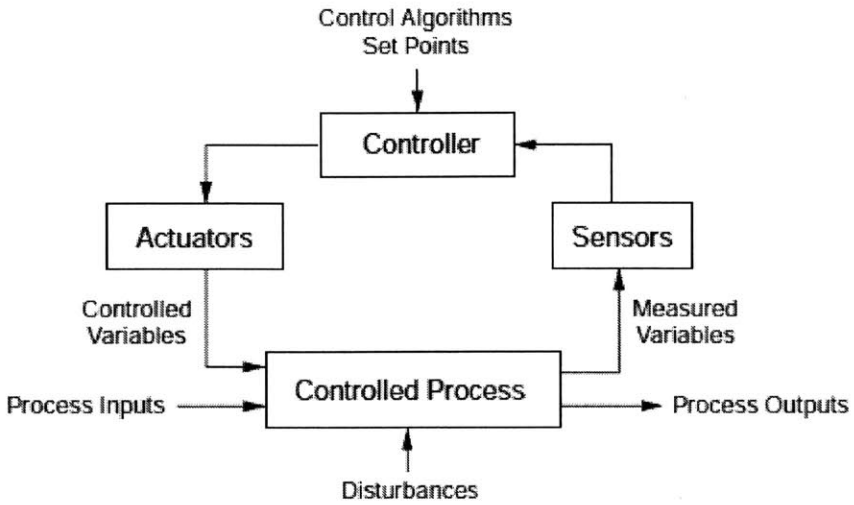


Figure 9.1.2: A Standard Control Loop [Leveson 2011]

9.1.3 Process Model

The third key concept in STAMP along with safety constraints and hierarchical safety control structures, is the process models. In control theory, four conditions are required to control a process [Leveson 2011, Leveson STPA]. In the context of STAMP, the four conditions are described in Table 9.1 below

Conditions for Process Control	STAMP context
Goal	Safety constraint that must be enforced by each controller in the hierarchical safety control structure
Action condition	Implemented via downward control channels in the hierarchical structure
Observability condition	Embodied in the upward(feedback) or measuring channels in the hierarchical structure
Model condition	Any controller, human or automated, needs a model of the process being controlled to control it effectively

Table 9.1: Conditions Required for a Control Process and Corresponding STAMP Context [Leveson 2011]

The process model, whether it's a mental model maintained by a human controller or an automated controller, must contain the same kind of information, namely the required relationship between the system variables (control laws), the current state (current values of the system variables) and the way the process can change the current state. This model determines what system variables need to be changed via feedback. If the controller's process model (human or automated) does not match the process, accidents can occur. According to Leveson [Leveson 2011], "Accidents often occur, particularly component interaction accidents and accidents involving complex digital technology or human error, when the process model used by the controller (human or automated) does not match the process". These variances manifest itself in the following four ways

- Incorrect or unsafe commands are given
- Required control actions for safety are not given
- Potentially correct control actions are provided at the wrong time (too early or too late)
- Control is stopped too soon or applied too long

STAMP can be used for both hazard analysis (ex-ante) as well as accident analysis (ex post) of systems. The goal of hazard analysis is to identify scenarios that can lead to losses or accidents. According to Leveson, hazard analysis can be described as "investigating an accident" before it occurs [Leveson 2011]. These scenarios can be eliminated or controlled in design or operations before they actually occur in a system. In STAMP, this type of hazard analysis is called STPA (System Theoretic Process Analysis) and it also includes causal factors that are not handled by older techniques. The second STAMP based method is used for analysis of systems after accident occurs. This type of accident analysis is called Causal Analysis based on STAMP (CAST) and

provides a framework to assist in understanding the entire accident process and identify the major systemic causal factors which led to the accident. The Target security breach will be analyzed with CAST and is the main objective of Chapter 10. The goal of CAST is not to identify just causal factors or variables, but it focusses on the entire socio technical system to identify weaknesses in the existing safety control structures in the system. CAST helps identify why the accident occurred and recommends changes to not only eliminate symptoms but also all the causal factors that led to the accident, potentially eliminating such accidents in future.

10: STAMP/CAST Analysis of Target Cyber Attack

"All urgent calls he shall hear at once, but never put off; for when postponed, they will prove too hard or impossible to accomplish." Book I "Concerning Discipline", Chapter 19 "The Duties of a King" - Chanakya's Arthashastra

In this section we will discuss the Target attack using the nine step STAMP/CAST framework. We have built on the framework used and previous work done for TJX STAMP Analysis [Cyber Safety CISL, Hamid 2014] as both of these breaches relate to stolen credit card data from large retailers.

10.1 Step #1: System(s) and Hazard(s)

System(s)

The Target cyber-attack occurred between Nov 27th and Dec 15th and during this time span, credit card data of about 40 million Target customers was stolen. Additionally, personal information of about 70 million Target customers was compromised [Elgin 2014]. Target's CEO and CIO were fired and the issuing banks incurred a loss of about $200 million. Target was subject to several lawsuits. The hackers had begun preparation and reconnaissance for some time before gaining a foothold in Target's systems in Sept 2013. For the next two months, they navigated within Target's systems installing malware and exfiltration software before eventually stealing credit card and personal data for over 110 million customers, in a span of just over 2 weeks and undetected. To understand how hackers exploited vulnerabilities within Target's systems and were eventually able to steal data of this magnitude, we will use STAMP/CAST analysis. In STAMP, the analysis beings with the system most proximate at the physical process level, where the accident has taken place. In Target, since the failure was loss of credit card data from POS systems, our system of focus will be the **Target Credit Card payment processing system,** which stored customer information and was used for processing customer purchases and returns at Target retail stores.

Hazard(s)

The hazard in question in the Target Credit card payment processing system is that **this system allows for unauthorized access to customer credit card and personal information details**. This unauthorized access can be non-malicious with no intent to do actual harm, however it can also be malicious, where the attackers purposely hacked the system to do harm.

10.2 Step #2: System Safety Constraints and System Requirements

System Safety Constraints

The System Safety constraints are listed below

- Target must protect customer personal information and credit card details from unauthorized access

- All warnings and alarms issued by the security systems must be looked at in a timely fashion and understood. If found to be legitimate, necessary, actions must be taken to fix issues and prevent recurrence. For e.g., in the Target case, the installed anti malware systems were functional and had fired alarms. It was Target's responsibility to evaluate and resolve these alarms in a timely fashion, however this didn't happen.
- Target must provide enough training to its security and IT staff to manage its technology infrastructure and keep them updated on the latest technologies and security controls
- Target must take measures to minimize losses from unauthorized access to its payment processing system. These include
    - It must immediately communicate with credit card payment banks about the access to minimize losses.
    - It must inform law enforcement agency and security experts and seek their help in minimizing the consequences of the attack
    - It must inform customers and provide support to them incase their personal information is breached.

10.3 Step #3: Target Hierarchical System Safety Control Structure

Broadly Target's system consists of two components: System Development and System Operations. System Development is relevant during the architecture and development of its IT systems, which includes Technology Strategy, specifications, vision etc. The System Operations part occurs when the system is implemented and rolled out and consists of day to day activities of the system. The safety control structures comprise of the roles and responsibilities of each component in the flow, along with controls for executing the responsibilities as well as feedback for gauging effectiveness of these controls.

The hierarchical system safety control structure of Target is shown in Figure 10.3 below. Only those parts of the system which are relevant for this analysis are described in the diagram. The bold dotted rectangle defines the **System Boundary,** and components within this boundary will be analyzed. For the purpose of this analysis, we have placed hierarchical control structures which have a direct impact or control on Target's IT systems, specifically security. These include systems all the way down to Payment Processing Systems, Security Management, Operations and Systems Management and Target Executive Management. The third party payment processing systems and external vendors have been kept outside the system boundary as there is indirect control and relationship with Target. It may be argued that the State Legislature and Congress should also be kept outside the system boundary, however as is increasingly evident today's Cybersecurity attacks are often led by renegade state sponsored attackers and they are not just an economic threat but a threat to freedom and national security. In such a climate, cybersecurity becomes shared responsibility of corporate and government alike. As such the governments have an increasing stake (manifested by control structures at highest level) in ensuring corporates conform to all security guidelines and best practices. The dotted boxes and arrows show the development part of the control structure, whereas the bold arrows and boxes indicate the operations part. The boxes indicate individual components of the system. The numbers represent unique loops representing control structure and feedback channels. The physical process is represented by a dashed oval and will be discussed in the subsequent sections. While exact details of Target's internal IT system architecture and implementation are not available in public domain,

the component nomenclature is typical of a large retail organization like Target [Cyber Safety CISL, Hamid 2014].

In the diagram, the bold loops (#10, #14, #15 and #16) indicate the interaction between development and system part. The first interaction (loop #14) is between Project Management and Operations Management which generates system requirements, RFP's and change requests. The feedback is provided by Project Management in the form of status reports. The second interaction is between Project Management and Third Party Vendor System (loop #10). This is a separate system which deals with managing access to Target Vendors like the HVAC manufacturer Fazio. In this case, the interactions consist of specifications, system requirements and processes while the feedback loop is in form of status reports and incidence reports. The third interaction is between Systems Management and Payment Card Processing System (loop#15) which consists of system testing, implementation and maintenance. The feedback consists of test results, logs and request for changes. Finally, the fourth interaction (loop #16), consists of interaction between Systems Management and Target retail store system. This includes technology support and a maintenance loop for all technologies related to retail store, post implementation and feedback is in form of reports and system logs.

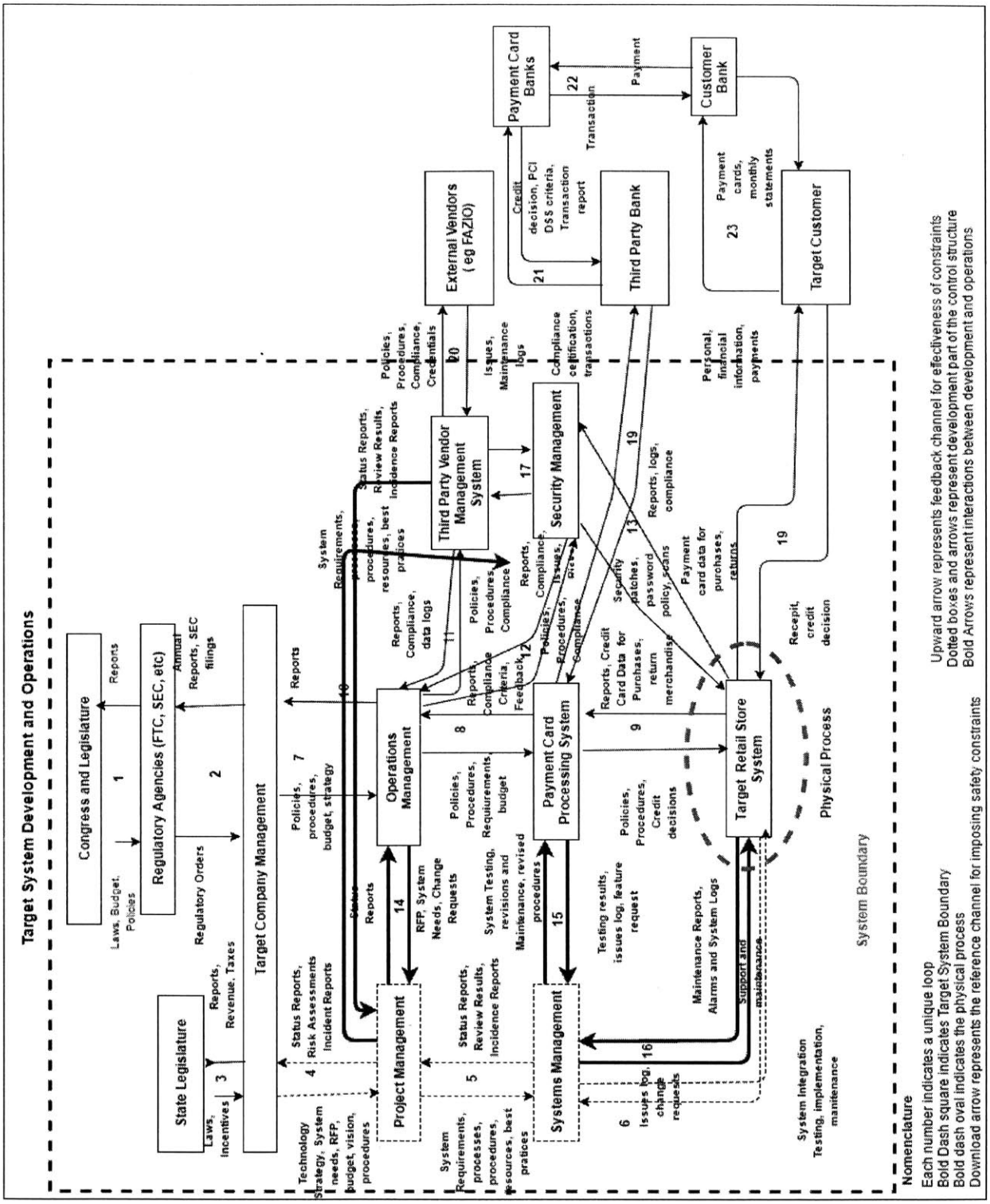


Figure 10.3: Target System Development and Operations Hierarchical Control Structure [Leveson 2011, Cyber Safety CISL, Hamid 2014]

10.4 Step #4: Proximate Event Chain

While the event chain does not provide the important causality information about the accident, in this case the Target cyber-attack, however the basic events which led to the attacks can be identified. This helps in gaining an understanding of the physical processes involved in the accident.

In a STAMP analysis, the proximate event chain includes a short time horizon. In case of Target, the attack was carried a little over four months from Sept 2013 to 15th December, when it was stopped. The Target case illustrate that while attack was started almost four months ago before it was finally detected, causal factors must have been in place much longer than that. The STAMP analysis will bring to light such causal factors in the remainder of the analysis. It must also be noted that while there must be several other issues in target IT systems, specifically in this analysis we are focusing on proximate events which led to Target's credit card and customer personal information loss at the physical process level.

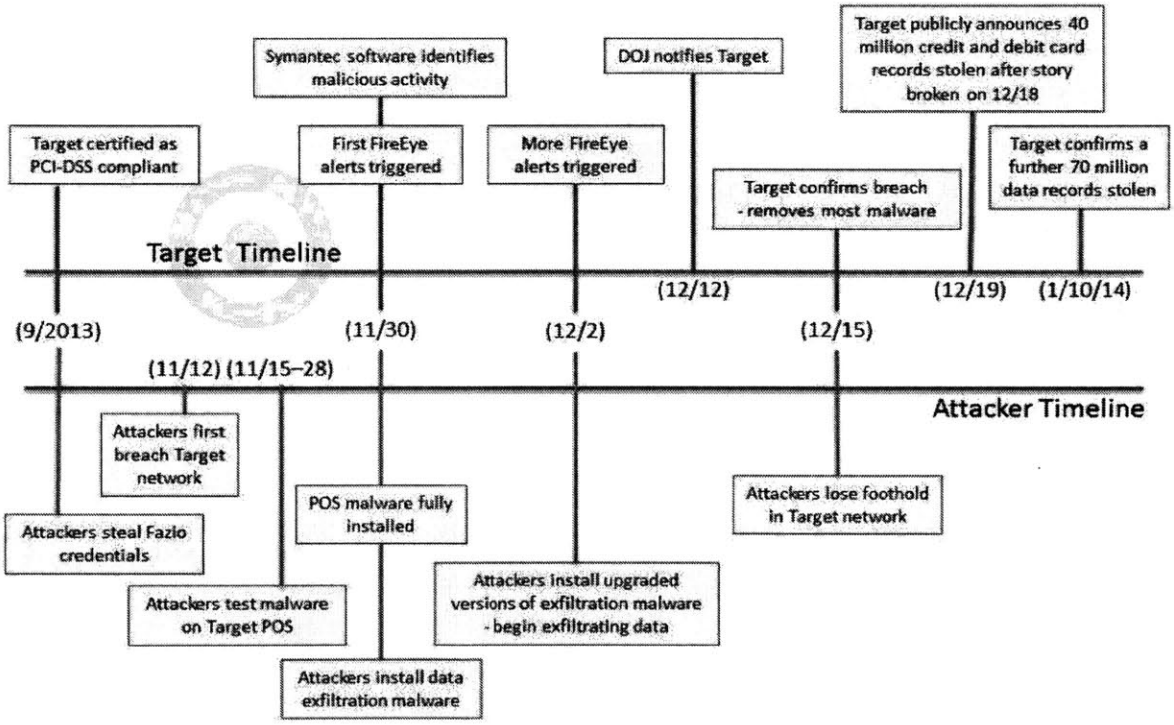


Figure 10.4 - Timeline of Target Attack [Kill Chain 2014]

The proximate events leading to the cyber-attack are summarized below. These events are based on the reports published by several organizations including Dell, US Senate Committee and several other independent researchers [Dell 2014, Kill Chain 2014, Aorato 2014]

- The hackers must have started with an initial reconnaissance survey. Not much is known about when exactly the hackers started their reconnaissance activities on Target's network, but it would have started with just a simple Google search. This reconnaissance would have revealed details about how Target uses Microsoft visualization software, centralized name resolution and Microsoft System Center Configuration Manager (SCCM) to deploy security updates and patches.
- Attackers then moved on to compromise target's third party vendor. Again the timeline of when it started, or how many vendors they targeted is not known, however in Sept 2013, they were able to compromise the credentials of Fazio Mechanical, an HVAC contractor. A phishing email was sent to Fazio employee allowing Citadel which is a variant of Zeus Trojan, to be installed on their computers.
- On Nov 12th, the attackers first breached Target's network.
- Later on 15th Nov, the attackers first tested their malware on Target's point of Sale systems (POS)
- On 30th Nov, the attackers fully install the POS systems. They then also installed data exfiltration malware on Target's systems. The first FireEye alert was also triggered the same day.
- On 2nd Dec, attackers also installed upgraded versions of the exfiltration malware and began to exfiltrate the data. More FireEye alerts were triggered.
- On 12th Dec, DOJ notified Target about the data breach in their systems. The dotted red oval in Figure 10.3 shows the physical process in the hierarchical control structure of Target's Retail Store System. The objective is to determine why physical controls were ineffective in preventing the system from transitioning to a higher risk state, eventually leading to cyber-attack. We shall look at several factors, including security policies, procedures, processes and compliance.
- On 15th Dec, Target confirms breach and removes most malware. Attackers lose their foothold on Target's network.

10.5 Step #5: Analyzing the Physical Process

Every IT system generally must have a three step tactical plan for prevention, detection and recovery against potential cyber-attacks. These are briefly described below:

Prevention
Firstly, every system should be safeguarded against attacks. These include firewalls, up to date antivirus and anti-malware software, data encryption, strong password requirements. These safeguards ensure basic defenses against cyber-attacks.

Detection
Anti-virus software is only as good as its dictionary and any new virus will not be detected. Similarly, passwords can be decrypted and accounts compromised. Therefore, the next step in

cybersecurity is to have good detection systems in place. These include tools that verify integrity of data and software and detect identity threat, malware and virus infections.

Recovery

Finally, if the system ends up being compromised, there should be speedy response to the attack. The infected systems should be isolated and then restored and rehabilitated quickly. The attack pattern should be understood and defense mechanisms must be placed to prevent such and similar attacks in future.

In this step, we shall analyze the losses at physical process level, through the context of prevention, detection and recovery.

- Identifying the physical and operational controls that contributed to the accident and analyze why they were not sufficient in preventing the system hazard
- Any physical failures that were responsible for the loss
- Were there any dysfunctional interactions and communication between the system and its components that contributed to the event?
- What were the unhandled external disturbances that led to the accident?
- What were the controls and mechanisms in place for detection and why where they not sufficient to detect the attack?
- What where the controls for recovery of the system after attack was detected and how effective were they?

10.5.1 Target Retail Store System

In this section, we will analyze the physical process Target Retail Store System. It consists of 5 control loops as shown in Figure 10.3. The Target customer interacts with the system through the Retail Store System, and it's the only point of contact with the system. The system processes credit card payment transactions and returns. (loop # 19). Customer buys merchandise from the store and present the form of payment (credit card, debit card). For returns, additional information such as driver's license may be required. In this section, focus will be only on purchase transactions, since it captures the personal information that was stolen by the attackers.

Target System acts on its customers by making credit card decisions (Target Store) either accepting or rejecting the payment card transaction for purchases (loop #19). A transaction is initiated by the customer by presenting a payment card at Target's POS (Point of Sale) terminal to make payment for purchases. The magnetic stripe at the back of the card contains unencrypted data about personal details of the customer and is read into the system by POS reader. This information is read into the volatile memory (RAM) of the system, unencrypted before transmission. The customer information is then transmitted by the POS terminal from Target store to the Payment Processing System (loop # 9) for credit decisions by customer's bank. The payment Processing system uses PCI-DSS standard which is proprietary data security standard for credit card companies. Since Target has recently passed the PCI-DSS audit, this implies that PCI-DSS compliance is not sufficient to ensure protection of credit card data.

The Payment Processing System also interacts with Security Management (loop # 10). The security controls implemented are general security of customer data, security patches/updates and strong passwords, while the feedback is provided in the form of reports and system logs.

10.5.1.1 Inadequate Control/Feedback

- **10.5.1.1.1 Security Management Capabilities (skills assessment and training)**

Attackers were successful in hacking Target store because there were vulnerabilities in the system. They were able to gain foothold into the system by stealing credentials of the HVAC vendor. They exploited web application vulnerability in "Ariba", Target's Billing System and uploaded a PHP file, disguising it as "xmlrpc.php". [Aorato 2014] The attackers were able to run arbitrary OS commands. The attackers then targeted Active Directory which contained data on all members of the Domain: users, computers and services. Once the attackers discovered the names of their targets including POS machines, they queried the DNS server to obtain the IP addresses. The hackers were able to obtain Domain Admin privileges by getting NT hash token commonly used in NT as a proxy to password. The hackers then created a new domain admin account by using functionality already provided in Windows. After that they were able to move to the less critical areas of the network to the more secure areas of the network and that too undetected and then propagated to the computers of interest using the new admin credentials. The attackers them installed malwares on POS to extract and then exfiltrate the data out of the network. It's clear that security there was lack of security skills assessment and training. Employees should have been made aware of the dangers of sharing critical system security information on the internet. Sensitive accounts should as that of Domain Admin should have been monitored for unauthorized use. The vendor information and Microsoft case study, with detailed the virtualization implementation about Target's systems and processes, should have been made available only on a need to know basis and not published on internet. Security management must ensure a holistic approach to system security which entails not just installing defense mechanisms, but also real time monitoring of critical systems as well as ensuring compliance.

- **10.5.1.1.2 Secure Network Engineering**

After gaining access, the attackers were able to move to the more critical areas of the network as they were not isolated from other areas of the network. Critical systems such as credit card payment systems should have been deeply segregated with tightly controlled access. Also several hardware systems including the domain controller were misconfigured making them vulnerable.

- **Data Encryption**

Although Target was following the PCI standards and passed the audit, it should have taken more measures to secure critical credit card data. This data was stored in raw format in system memory, without any encryption making it vulnerable to theft. By using point to point encryption (P2PE) for POS Systems, Target would have greatly reduced risks of customer information getting stolen. Target could also have used Hardware encryption devices directly tied to the pin pad to eliminate the need of keeping credit card information in memory [Gomzin 2014].

- **Network Monitoring and Alarm Resolution**

After gaining access to Target's network, the hackers moved around the internal systems virtually unnoticed. Hackers undermined several of Target's internal servers and moved laterally within the system. When the attackers were installing malware on Target's internal systems, its monitoring software FireEye issued several alarms and notifications. However,

Target failed to take any action after these events. The exact reason for inaction is not known, however one plausible explanation could be that the IT team was overwhelmed by the number of daily security alarms issued and they did not have mechanisms in place to filter and prioritize such alarms and not have enough resources for quick resolution. Target had close to 2000 stores and on an average 30 POS per store, besides a host of internal systems, so it could have been possible that its security monitoring team was simply overwhelmed by the number of alarms it was receiving.

- **Third Party Access and Vendor Management**
  Hackers were able to exploit vulnerabilities in Target's vendor management system. Hackers were able to install malware through an email sent to Fazio Mechanical employee and stole its security credentials. Target should have highly controlled access by its third party vendors which could have included two factor authentication, training to let vendors keep their systems updated with latest patches of anti-virus, as well as application firewall to monitor and scan for vulnerabilities and unusual activity.

Safety Requirements and Constraints Violated:

- Target must protect customer personal information and credit card details from unauthorized access

Emergency and Safety Equipment (Controls):

Target had several controls and security measures in place to prevent unauthorized access to their systems:

- Login credentials/authentication for third party vendors for gaining access to Target's vendor management system
- Following PCI protocol for customer credit card processing systems
- Malware monitoring software, FireEye installed in internal systems for real time detection of spurious activities
- Login credentials for BMC's performance Assurance software for Microsoft Virtualization Servers.

Failures and Inadequate Controls:

- Attackers stole the credentials of Fazio mechanical, a third party HVAC vendor. They were successful in breaching into Fazio's computer system as there were insufficient security controls in place. The computers were not installed with the latest patch of malware software and the employees were not trained enough or had awareness on against malware. Besides Target did not have any procedures in place to ensure its third party vendors use updated versions of security software. Target also did not have dual authentication in place, so once hackers got access to the login details, they were able to connect to its systems.
- While Target did comply the PCI protocol and passed the audit, it should have shown more caution in managing the most sensitive customer information including credit card details. This data resided in system memory in raw format. Target should have used some form of encryption while storing this data.

- After hackers joined the store, they were able to move laterally within the system but their presence was not detected by Target. There were no security tools or periodic scans done to gather data about unusual activity or active connections. Target should have had real time active defense mechanisms in place. Days after the attack, Target asked security experts at Verizon to probe its networks for weaknesses. According to the findings of Verizon's report [Krebs 2015], *"no controls limiting their access to any system, including devices within stores such as point of sale (POS) registers and servers."*
- While Target had a password policy, it was not being followed [Krebs 2013]. A file containing valid network credentials was stored on several servers. The systems and services utilized either weak or default passwords. Default passwords in key internal systems and servers also allowed the Verizon security experts [Krebs 2015] to get system administrator access with freedom to move about Target's massive internal network.
- Several services and systems also had either outdated or missing critical security updates. Even high profile patches were not updated leaving several key systems exposed to vulnerabilities. Target hasn't publicly shared the reason for such inaction; whether it was human error, culture of complacence or lack of follow up mechanisms.
- Target had a comprehensive system vulnerability scanning program in place, however the Verizon report observed that there was a disconnect between the vulnerability program and the remediation procedures rendering the program essentially ineffective.
- Incorrect implementation/maintenance of processes and security procedures at the physical process level.
    - The weakness in monitoring or implementation could be due to missing processes, inadequate training, documentation or checklists.
    - Insufficient mechanisms or controls in place to monitor alerts and warnings issued by anti-intrusion software. It was reported that FireEye issued multiple flags when malware and data exfiltration software was being installed, however no action was taken by Target
    - DLL name was generic [winxml.dll] and the installed process also had a generic system service name to mask its identity [Dell 2014]

Physical Contextual Factors:

- Target's vision of "Expect More, Pay Less", drove many of their business decisions. In order to reduce costs, improve infrastructure management and increased system availability, Target migrated to Windows Datacenter and Hyper-V virtualization for all its stores, resulting in millions of dollars of savings. It could be possible that in its drive for cost cutting in IT, Target overlooked the security aspects of making these changes leaving its systems exposed to cyber threats. As systems were integrated and consolidated, it also increased the threat profile of the IT systems. Without sufficient security controls in place, an attacker could easily navigate from less critical areas of the system to more critical areas. Target also failed to provide barriers to more sensitive areas of their systems. The hackers were eventually able to gain access all POS terminals within Target and install malware. The Verizon report in the aftermath of the attack [Krebs 2015] lists several vulneraries in the Target system including default passwords in key internal systems and servers, missing critical patches and running outdated software during their external penetration test.

- Target had recently been certified PCI compliant. This could have given them a false sense of security, assuming that credit card data was not secure. Companies often times reduce the scope of PCI audits in order to pass them, as they are mainly seeming as an apparatus by which issuing banks make money by levying fines if standards are not followed.
- Assuming that security team had activated the monitoring at the physical process level, it could be that Systems Management process for selecting and prioritizing the monitoring alarms was very tedious. Target had over 1800 stores in 49 states and an average of 30 POS systems per store, so gathering data and scanning system log files, and respond quickly could be a challenge. It's likely that the cybersecurity team within Target would receive tens of thousands of security alerts per day, from its large number of POS and other internal systems and simply didn't have the bandwidth or resources to resolve these timely.

Figure 10.5 CAST analysis of Target System – Physical Process Level

10.6 Step #6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

In previous step, we identified four control/feedback inadequacies at physical process level which lead to weakening of defense mechanisms with Target, and ultimately led to stealing of customer data. The first was storing credit card data unencrypted within the memory of POS system. Secondly security protocols (strong passwords, and malware patches) were not followed by employees and even several critical systems had weak or default passwords. Thirdly the Vendor Management System did not have adequate safeguards in place (e.g. dual authentication) and were not isolated from the rest of the critical systems. Lastly in spite of alarms being issued by FireEye, no action was taken to either analyze or stop the attacks. Although Target's Bangalore Team responded and notified the IT team in Minneapolis, no further was action was taken. To understand why these shortcomings existed, we need to analyze both the development and operational components at higher levels of Target's hierarchical safety control structure. According to STAMP framework, in order to understand behavior of any levels of a socio technical system, we need to investigate at the higher level.

10.6.1 Payment Card Processing System

One level up from the physical process from Target's hierarchical safety control structure, is the Payment Processing System (loop # 9). The Payment System is responsible for maintaining the safety of customer data and also transmitting customer credit card decision to external bank upon receiving information about purchase and payment information. If the external bank approves the request, it processes the transaction internally within Target's systems. Customer payment card data requires to be stored on Target's servers according to PCI-DSS specifications. The customer information is also stored within Target's servers for merchandise returns. It is also responsible to ensure compliance with PCI-DSS.

A key requirement of the Payment Card Processing System is to maintain integrity and safety of customer data. This is shared responsibility of this system along with other components of the

control structure. The payment Card Processing also interacts with Systems Management (loop # 15) for systems testing, maintenance and enhancements. The feedback is provided in terms of system testing, reports and system logs. This link ensures that this system meets the internal specifications, standards and Target's policies while also complying with PCI-DSS, including safe storage of customer data in memory.

Payment Card Processing System and System Management
Among the several issues were customer credit card data was stored encrypted in memory. The critical systems did not have latest malware protection or strong passwords as well as alarms were ignored. Besides the critical systems like payment card processing were not secured. For PCI-DSS, it could be that the requirements were not correctly communicated or only the bare minimum were asked to be implemented. All these will have to be looked in detail by analyzing higher level components in the hierarchy.

Inadequate control/feedback
When the attack happened, Target was in compliance with PCI-DSS standards and had passed the audit. According to PCI-DSS guidelines, credit card data should be encrypted but it did not enforce this requirement.

Compliance with PCI-DSS
Target was fully in compliance with PCI-DSS.

Safety Related Responsibilities

- Ensure that customer personal data, especially credit card information is encrypted during the transaction process. This includes data that it being stored temporarily in the computers RAM
- Ensure that all payment card transactions conform to the PCI-DSS standards
- Ensure that all POS terminals and related systems have strong passwords, latest anti-malware protection and comply with the security guidelines defined by Target

Context
When the Target cyber-attack happened in 2011, Target had passed the PCI-DSS compliance audit. However, customer credit card information still got stolen. It was later discovered that the malware had scrapped unencrypted data from the memory and many passwords with either too weak or were default passwords. Besides latest anti-malware software had not been installed on POS.

Unsafe Decisions and Control Actions

- Hackers exploited weaknesses in Target's IT systems and the way credit card data was processed.

- Point to Point encryption was not used, although compliance with PCI-DSS, while handling customer payment data.
- Sensitive and critical systems like credit card payment systems were not sufficiently isolated from the rest of the IT systems
- Security policies were not strictly enforced. Employees had weak or default passwords and latest security patches had not been installed.
- Target had also stored personal information of its customers, possibly for handling return merchandise

Process Model Flaws

Assumption by Target that adherence to PCI-DSS standards is sufficient for ensuring safety of customer payment info.

Figure 10.6.1 CAST Analysis of Payment Card Processing System

10.6.2 Security Management

One level up the hierarchy in the control structure is the Security Management. One of its major responsibilities is to ensure the safety and security of all Target's systems, especially the critical systems. It also defines and enforces password policies, sends security patches and periodic scans and monitors systems (loop # 13) and ensures compliance by collecting reports and logs (loop #19).

Interaction between Security Management and Retail Store System

Since Target's employees were not in compliance with the security guidelines and systems were out of date with regards to malware installation, the controls in the loop #19 were not effective and sufficient. Moreover, after the attackers installed malware, several alarms were flagged by the intrusion detection system, however no action was taken. Lack of management emphasis and controls or inadequate monitoring seems to be responsible for weakening of this loop. The CAST analysis of Security Management is given below

Safety Related Responsibilities

- Develop and communicate system security related policies
- Ensure compliance with all security related protocols and requirements
- Provide resources for proactively responding to security alarms and resolving them

Context:

- Target had expanded rapidly during the decade and had almost 2000 stores at the time the accident happened.
- There may not have been enough emphasis to follow through on the security measures, assuming that the perimeter defense (e.g. firewalls) was sufficient.
- There as a major push for virtualization and operational and cost efficiency which may have led to lower emphasis or budgets for security management.

Unsafe Decisions and Control Actions

- Not following up and strictly enforcing password and security updates policy.
- Even after several alarms were raised by FireEye, not investigating the issue in a timely manner or taking measures to safeguard the systems.

Process Model Flaws

- Lack of understanding of how vulnerable internal systems would be without strictly enforcing security policies.
- Assuming PCI-DSS compliance is enough to guarantee the safety of customer data.
- Lack of understanding of how exposed the critical systems were, once a hacker was able to gain access to the system.

Figure 10.6.2 CAST Analysis of Security Management System

10.6.3 Third Party Vendor Management System

The Third Party Vendor Management System was responsible for managing interaction with Target's external vendors. These vendors provided services to manage Target's infrastructure and billed Target for such services. Fazio Mechanical was one such vendor. This system would provide login credentials, communicate policies and procedures to the external vendors (loop # 20) and ensure compliance and resolve issues through the control feedback (loop # 20). Since attackers were able to steal credentials from Fazio and then gain access to Target's systems and move around laterally into its systems unnoticed, it's evident that some security controls were not enough. The CAST analysis is give below.

Safety Related Responsibilities

- Ensure compliance of Target's security policies and policies
- Provide secure access to the vendor management system

Context:

- Target is a large retail store chain operating in 49 states at the time of attack. As such it must have a large number of external vendors.
- It underwent rapid expansion during last several years.
- Target's IT department had emphasized virtualization and consolidating and economizing IT services in order to be efficient and be aligned with "Expect More, Pay Less" brand promise.

Unsafe Decisions and Control Actions

- Having insufficient security credentialing for vendors. Could have used two step authentication.
- Not ensuring that the vendors had latest malware software installed in the systems. Since these vendors are outside the system boundary, there are practical limits on however Target can enforce its security policies.
- Not having measures in place to detect spurious activity. Hackers were able to move around from the vendor management system to other systems in the network.

Process Model Flaws

- Underestimating the importance of having strict security controls in place for vendor management system.
- Assuming the vendor management system is disconnected from critical systems within the network.

Figure 10.6.3 CAST Analysis of Third Party Vendor Management System

10.6.4 Operations Management

One level up in the hierarchical control structure is the Operations Management. In the present context, the role of operations management is to provide processes, procedures and policies for handling securely customer information, managing customer data which includes retention, disposal and archival, ensuring compliance with PCI-DSS as well as budgets and necessary resources to implement the policies.

Safety Related Responsibilities

- Develop and communicate policies for customer information and vendor management systems.
- Ensure compliance of defined payment card related as well as vendor management policies and procedures.
- Provide necessary resources to implement and maintain these systems.

Context:

- Target was in a phase of rapid expansion during last few years and had presence in 49 states in US and was also expanding in Canada.
- Focus may have shifted to develop operational efficiencies and cost effectiveness in the IT systems.
- Since Target had passed the PCI-DSS audit, it may have led to false sense of security.
- It may have felt that maintaining regular security controls like patches and strong passwords was not something which needed to be emphasized in the audit reports

Unsafe Decisions and Control Actions

- Not placing security measures for critical systems and separating them with non-critical systems.
- Lacking robust controls to measure and audit whether security policies were being followed and enforcing compliance.

Process Model Flaws

- Assuming compliance of PCI-DSS standards was sufficient to guarantee safety of customer data and is just a technology issue.
- Leniency in enforcing security controls throughout the organization, especially those dealing with critical systems.

Figure 10.6.4 CAST Analysis of Operations Management System

10.6.5 Target Companies Management (System Operations Part)

The next level up in the control structure is Target Management. It defines and controls and defines company policies, plans, procedures, strategic initiatives and budget. With reference to Payment Card processing and Vendor Management System, it is responsible for audit recommendations, ensuring security of customer data, securing third party vendor systems, and ensuring that all security guidelines established are enforced. It is also responsible for that the security infrastructure is robust and well-funded. Additionally, Target Management is also responsible for ensuring compliance with all State and Federal laws and regulations. The Target Management allocates budgetary resources and defines priorities. The feedback is in form of reports (loop # 7). The CAST analysis of Target Companies Management is given below.

Safety-Related Responsibilities:

- Ensure compliance of all State, federal laws and regulations as well as industry standards.
- Allocate enough resources and implement enough measures to ensure that all policies, procedures are implemented and followed.

Context:

- The rapid expansion of Target in recent years may have shifted focus to develop operational efficiencies and security measures may not have been able to scale up accordingly.
- In its constant endeavor to deliver value to customers, Target may have focused on bringing costs down through virtualization of servers and consolidation of IT systems, without paying similar emphasis on security. While this helped bringing costs down, it may have helped move the systems to a higher risk state.
- There was no executive management role for security and risk management.

Unsafe Decisions and Control Actions:

- Lack of policies or placing sufficient emphasis at executive level on securing personal customer information.
- Being unable to develop and nurture a culture of security and safety within the organization.
- Lack of processes and policies for measuring and evaluating adherence to internal security guidelines for systems and employees.

Process Model Flaws:

- Inadequate understanding of the cybersecurity risks faced by large retailers like Target.
- Insufficient communication of top level priorities with reference to managing critical systems and protection of customer data
- Lack of emphasis on security management and infrastructure.
- Lack of accountability with regards to adherence of security measures and guidelines.
- Lack of awareness on the latest happenings in the cybersecurity area and threat level faced by large retailers.

Figure 10.6.5 CAST Analysis of Target Companies Management (System Operations Part)

10.6.6 Regulatory Agencies

The next level up in the control structure is the role of regulatory agencies. They enforce laws which are passed by the congress and address complaints made by consumers against businesses (e.g. inadequate protection of consumer data), give directives to businesses if they are not complying and investigate businesses if there is a breach of customer data. Feedback is provided by Target Company Management by submitting annual reports, SEC filings and responding to investigations (loop # 2).

At the time of attack, Target was in full compliance of PCI-DSS and there was no reported directive issued by the regulatory agencies. The CAST analysis is given below.

Safety-Related Responsibilities:

- Ensure that companies are aware of their responsibilities with reference to securing personal customer information.
- Ensure full compliance with laws and regulations passed by the government.

Context:

- There is no central organization which defines and mandates cybersecurity standards. As such implementations can vary.
- The widely used standard for securing customer payment info PCI-DSS, proved to be insufficient in ensuring security.

Unsafe Decisions and Control Actions:

- Inadequate regulations by governing bodies with reference to securing personal customer information.

Process Model Flaws:

- Since today's IT systems are very complex, it's hard to detect when an intrusion is occurring. Both systems as well as attacker's methods are continuously evolving making it hard for regulatory bodies to identify regulatory weaknesses and adapt quickly in face of cyber-attacks.

Figure 10.6.6 CAST Analysis of Regulatory Agencies

10.6.7 State Legislature

The Minneapolis state legislature also controls Target's Management by enacting laws and provide incentives for businesses to stay competitive and help in expanding the economy. It receives feedback through reported (loop # 3).

Safety-Related Responsibilities:

- Pass laws and regulations to protect customer payment information.

Context:

- Target is headquartered in Minneapolis and contributes to local economy by way of jobs and taxes.
- The State legislature has to encourage companies like Target to stay and expand and being business friendly while at the same time enforce rules and regulations. This can be a tricky balancing act.

Unsafe Decisions and Control Actions:

- Lack of enough oversight or understanding of security issues faced by large retail industries.
-

Process Model Flaws:

- General lack of understanding in regards to what regulations to pass in order to stop Target type cyber-attacks.

Figure 10.6.7 CAST Analysis of State Legislature

10.6.8 Congress and Legislature

The Congress and Legislature is the highest level in the control structure. It passes broad regulations and structure for industries and businesses to operate in the country and receives feedback through its regulatory agencies (loop # 1). The US government is actively involved in

the subject of cybersecurity. During the Target breach, the DOJ and secret service investigated the cyber-attack. The CAST analysis is given below.

Safety Related Responsibilities

- Protect the nation's interests against cyber-attacks.
- Enact laws and regulations to persecute cyber criminals.
- Provide resources to help prevent cyber-crimes.

Context:

- There are lobbyists who want less government control and regulation
- Cyber criminals can launch attacks from anywhere in the world, especially from unfriendly countries, making it difficult to investigate attacks and prosecute cyber criminals.

Unsafe Decisions and Control Actions

- Inadequate laws and regulations with respect to payment card security standards.

Process Model Flaws

- None.

Figure 10.6.8 CAST Analysis of Congress and Legislature

10.6.9 Systems Management

The other side of the control structure has Systems Management, which controls Target's Retail Store System (physical process) technology infrastructure (loop # 6). It executes control by way of systems integration and testing, feature implementation and gets feedback in the form of report logs and change requests. There's a second loop (#16) for support and maintenance of systems and feedback is in the form of maintenance reports, alarms and system logs. The CAST analysis is summarized below.

10.6.9.1 Inadequate control/feedback

10.6.9.1.1 Monitoring of Internal Network

Most companies have monitoring processes within the internal networks to identify suspicious activities if any. In Target's case, it appears that hackers were able to go unnoticed and moved laterally across many systems including the high security ones. Changing the configurations of systems requires administrative privileges and it appears that the hackers were able to have access to the credentials. The hackers installed malware into POS terminals and also later to exfiltrate the raw data. Although alarms were raised by FireFly, no action was taken against these incidents. Lack of sufficient monitoring in the internal network contributed to weakening controls and inadequate feedback.

10.6.9.1.2 Security Technology Operations

The CAST analysis revealed that some of the critical internal controllers and systems had outdated malware installations and default passwords. The Systems Management was responsible for implementing and maintaining this technology. The likely cause is lack of proper training and enough awareness about how to manage security technology.

10.6.9.1.3 System Maintenance

Target had the policy of installing latest malware software on the systems. The system also triggered alarms when malware was installed on their systems. Part of system maintenance was to monitor the security logs and alarms and take corrective action. The CAST analysis is given below:

Safety Related Responsibilities

- Understand the loopholes or weaknesses in the current security management infrastructure and communicate to senior management about ways to mitigate these.
  This include securing the most critical areas of the system and implementing enough security around it to safeguard these systems as well as having enough resources to monitor system alerts.

- Implements Target's security policies and guidelines as per the requirements:
  - Policy for password strength.
  - Schedule and compliance of security software installations
  - Monitoring of Target's Internal network for unauthorized usage.
    - Implies unauthorized connections and data usage or unusual data traffic.
    - Must monitor account id's and the processes run by these. E.g. only authorized account should be allowed to install software on POS systems.

Context:

Target had about 1900 stores each with approximately 30 POS terminals and other supportive systems. To have timely and robust response to every security alarm is an extremely complex task and requires resources.

Unsafe Decisions and Control Actions

- Inadequate or insufficient monitoring of internal networks.
- Weak policies and controls for passwords for system admin accounts
- Lack of accountability for quickly responding to safety alarms
- Inadequate monitoring of Target internal systems for unauthorized usage and installation of malicious software

Process Model Flaws

- Lack of adequate understanding about securing customer payment data. As the CAST analysis of physical process reveals, there was apparently a belief that compliance to PCI-DSS is a necessary and sufficient condition for securing payment data. Having raw credit card data in memory of internal systems of Target's systems might have deemed to be low risk.

- Lack of correct process or checklist for securing and managing the security technology infrastructure.
  - Many of Target's servers and terminals had outdated malware and weak passwords, indicating systemic faults in enforcing security policies.

Figure 10.6.9 CAST Analysis of Systems Management

10.6.10 Project Management

One level up the control hierarchy of the development part, is the Project Management. It controls Systems Management (loop # 5). Project Management communicates the system requirements, processes and procedures, best practices and provides necessary resources to complete the projects. Feedback is obtained by way of status reports, review of results and incidence reports, system performance, technology assets inventory and status of existing technology infrastructure and requests for upgrades. The CAST analysis of Project Management is summarized below.

Safety Related Responsibilities:

- Emphasize implementation of all PCI-DSS standards to ensure safety in design of payment card processing systems.
- Provide adequate training of IT professionals for maintaining and operating security technology infrastructure.
- Conduct periodic reviews of security infrastructure and ensure all documentation is current and up to date. Ensure latest security practices are incorporated in day to day workings of IT staff.
- Evaluate audit reports with respect to compliance of security practices within the organization and take necessary measures to address gaps and shortcomings.
- Perform rigorous of system testing to ensure all system design goals are being met.

Context:

- Project Management just like Security is a cost center because it has a supporting role and does not directly contribute to bottom line. As such acquiring funding is always a challenge. Having less resources can lead to incorrect security risk assessment or de-prioritization of security related initiatives for lack of funding.
- Inadequate executive management support for implementing security features (e.g. having additional security layers for critical systems).
- Target passed PCI-DSS audit and this may have led to a false sense of security and being immune to cyber-attacks.

Unsafe Decisions and Control Actions

- Decision not to isolate the more critical systems from other non-critical systems within the organization.

- Inadequate understanding of PCI-DSS and the pitfalls of saving customer payment in raw format in memory.
- Either lacking resources or not providing priority to resolve all alerts in a timely fashion and developing a culture of responsibility and accountability.
- Not exercising enough control on what documents should be made publicly available. Several reports detailing the implementation of Microsoft's Virtualization solution were published on the internet.

Process Model Flaws

- Lack of or inadequate awareness on understanding of sensitive customer payment information.
- Inadequate knowledge of the latest threats emanating in cybersecurity, particularly in the retail industry. The US government had already issued several warnings of new types of malwares and hackers had actively been collaborating on sharing information about malware tools being developed.

Figure 10.6.10 CAST Analysis of Project Management

6.6.11 Target Companies Management (System Development Part)

The next level up is Target Companies Management. It controls Project Management and is responsible for laying out broad system needs, request for proposals, procedures, overall technology strategy and provides budget for Project Management, it exercises control by way of status reports and reviewing results and addressing any concerns or issues flagged (loop # 5). Among Target Senior Management, The CIO is mainly responsible for managing this relationship with Project Management. The CAST analysis is provided below.

Safety Related Responsibilities

- Ensure compliance of technology regarding retail industry standards and procedures.
- Ensure that technology solutions fulfil the business needs of Target.
- Make sure that measures are implemented to secure critical information technology assets against cyber threats.
- Drive a culture of safety and accountability across all levels within the organization.

Context:

- CIO is generally always under pressure to keep costs down while ensuring business needs are met.
- Rapid expansion of Target stores led CIO to take measures to bring down operational costs and achieve greater efficiencies
- No dedicated role in executive leadership to address cybersecurity risks. CIO has responsibility to manage all technology issues including cybersecurity.

Unsafe Decisions and Control Actions

- Safety culture not enforced top down. While Target had invested in developing processes and tools for preventing cyber-attacks, a culture of less accountability ensured that its systems were very vulnerable to these attacks.
- Lack of communication and support in relationship to securing critical systems company wide.
- Either not providing enough support or resources at executive level, or not ensuring accountability in order to address issues when security alarms were flagged.

Process Model Flaws

- Not having enough understanding about the scale and scope of risks associated with large companies like Target.
- Not understanding that to safeguard against cyber-attacks, just PCI-DSS compliance is not sufficient.
- Inadequate knowledge of latest cybersecurity risks specifically within retail industries
- Lack of understanding on the role of individual accountability of employees to manage external cybersecurity risks.

Figure 10.6.11 CAST Analysis of Target Companies Management (System Development Part)

10.7 Step #7: Coordination and Communication

- The CAST analysis has revealed several areas of coordination and communication weaknesses that led to Target cyber-attack.
- The Payment Card Processing System is controlled by Operations Management (loop # 8) and interacts with the Third Party Bank (loop # 19). The Third Party Bank relies on Target to comply with PCI-DSS requirements and keep customer data safe. The processing system also interacts with Target Retail Store System (loop # 9). Target had passed the PCI-DSS audit few months before the attack took place. Although in PCI-DSS standard, it was recommended that customer card data should be encrypted with stored in RAM, Target did not implement this and stored raw data in memory. It can be inferred that it was assumed that passing PCI-DSS audit was sufficient to guarantee safety of customer data and there was not enough impetus by senior management to do more than minimum compliance. There was also lack of communication and coordination during the development cycle in fully securing point to point encryption, which could be either lack of understanding or insufficient emphasis placed on customer data security.
- The risks of keeping raw, unencrypted customer data were not communicated effectively at the senior and executive level. Although is a very large retailer with customer data in hundreds of millions, there was no dedicated role for managing cybersecurity risks within the company. As such, cybersecurity risks were not actively communicated and managed.
- There were many internal systems which had weak passwords and outdated anti-malware, including even critical systems. This clearly points to lack of coordination between the

Security Management and Retail Store System (loop #13). Either the requirements were not emphasized strongly or there was no follow up or coordinated effort to ensure that people and systems are compliant with security guidelines. This could also point to laxity by Senior Management in communicating the significance to keeping systems secure and nurturing a culture of safety.

- Target had launched major initiatives in the last few years to rely on virtualization of its servers and internal IT systems with help of its partner, Microsoft. This was intended to lower costs, increase efficiency and system availability and ultimately deliver value to its customers. However, after going through company's memos and reports during that period, there was clearly lack of similar emphasis at the senior and executive level in enhancing security measures. It could be that there as a misunderstanding that existing measures are sufficient or the management lacked awareness of how integrated systems can expose the organization to a higher risk state. The communication seems to be lacking at executive level, most likely due to lack of focus, different priorities and risk awareness.
- It is plausible that the CIO was prioritizing budget to achieve operational efficiency and cost effectiveness and security was not pursued with the same rigor. The fact that critical systems did not have additional security layers to protect sensitive information, clearly points to lack of priority given to safety. Since CIO is a cost center and not revenue generating center, therefore there are limits to CIO's influence within executive leadership.
- There could also be lack of communication between CIO and the Security Management staff. Guidelines and expectations must not have been clearly communicated and prioritized. The fact that even after alarms were flagged by malware detection software, no action was taken, clearly also point to communication and coordination issues within the company.
- The Third Party Vendor Management System also did not deploy Dual Authentication or had capability to detect spurious activity. This also points to lack of communication and coordination with Security Management (loop #17).
- Target also seemed to lack a centralized knowledge database which had security requirements and guidelines as well as newer risk threats emanating specifically in retail industry. This could have led to higher risk awareness and more proactive steps taken to mitigate weaknesses within the systems and also led to higher compliance.
- Lastly another coordination and communication issue was related to Systems Management which is responsible for Systems Integration, testing, Implementation and maintenance at the physical process level. The CAST analysis of the physical process level revealed weak controls and they can be attributed to lack of coordination and communication between implementation and maintenance teams.

10.8 Step #8: Dynamics and Migration to a High-Risk State

Many major accidents happen as a result of migration of a system to a higher risk state over time [Leveson 2011]. By properly understanding the dynamics of migration, one can help redesigning the system to lower the risk state. The CAST analysis discussed above pointed to some operational and behavioral aspects that ultimately contributed to Target cyber-attack.
A major factor contributing to the cyber-attack was Target's move to Virtualization [Target 2011]. Earlier Target had dedicated two servers [Microsoft 2011] for each store but as it was expanding rapidly and opening more stores it required an alternative solution to manage its IT infrastructure. Target partnered with Microsoft to implement virtualization solution. This helped reduce operational cost by minimizing the physical infrastructure at each store and resulted in savings of millions of dollars in hardware, electrical and maintenance cost. This solution offered several benefits and was deemed a success both by Microsoft and Target.

Operational efficiency and cost optimization seemed to be the driving force in IT department but probably security was not given similar emphasis and assumed to be sufficient. Here are some quotes from senior management at Target before the attack happened. [Target 2011].

- *"Virtualization had become a viable alternative to simply deploying more servers. It also would allow us to make better use of existing server capacity and reduce infrastructure management"* - Brad Thompson, Director of Infrastructure Engineering, Target

- *"Our Microsoft Virtualization solution is an essential part of Target's strategies for consolidating and economizing IT services at our stores"* - Fritz DeBrine, Senior Group Manager, Server Technology and Enterprise Storage, Target

These quotes clearly indicate that economizing IT was a priority at that time. It is plausible that security did not receive a similar focus.

Most of Target's 1900 stores and over 30000 POS stations [Target 2011] were integrated as part of this solution and it became easier to maintain these systems and several routine tasks were automated. Implementing Virtualization, while not paying sufficient attention to understand the security ramifications also providing additional security to its systems, resulted in these systems becoming increasingly vulnerable to threats. Microsoft had also published several technical papers describing the details of the implementation and posted them on public domain. The hackers had access to these reports and could easily decipher system vulnerabilities. In the new virtualized setup, Target had not provided security covers to the critical systems or separated them, so a hacker could pretty much move laterally within the system once it got a foothold inside it.

Lack of understanding about the risks involved with storing raw customer data also proved to be a critical error on Target's part. It did not implement all of PCI-DSS recommendations regarding handling customer payment data.

Target had a large number of vendors and in order to automate the billing and payment systems, it had created a vendor management system. While the goal was improving and streamlining

processes, not separating this system from the other parts of its IT infrastructure was also responsible for the movement to high risk state.

In the last decade, the hackers were also getting increasingly sophisticated and had developed a cyber ecosystem, which included sharing information on forums, blogs etc. and developing sophisticated tools to hack systems and steal information. Target did not have a dedicated role to manage such security risks and take proactive action. This inaccurate risk assessment also led to Target moving to a highly vulnerable state.

Target was in full compliance with PCI-DSS which could have led to confirmation bias. It might have given it a false sense of security and assumed that all its payment data was completely secure. Companies need to constantly reevaluate it security infrastructure and adapt to the new and unforeseen challenges.

There could also be a culture of complacency as related to the security of its internal systems. Since most employees did not follow security guidelines, systems had out of data malware detection software and no action was taken, this points to a general lack of safety culture. As systems become increasingly integrated and processes automated, this also helps to move things in a higher risk state over time.

Although FireEye had detected malware installations and sent out alarms, the issue was not investigated and no follow up action was taken. It could be that Target had not invested in developing processes and procedures to manage the security alarms and take action. The security infrastructure might have lacked the resources to investigate and take action on the massive amounts of data being generated. The rapid expansion of Target stores and increased automation and integration of IT processes, coupled with lack of similar emphasis on security, also helped move the systems to a high risk state, leaving it vulnerable to cyber-attacks.

10.9 Step #9: Recommendations

Based on the STAMP/CAST analysis in the previous sections, the following are the key recommendations that companies like Target can use to manage cybersecurity risks and prevent such similar attacks in the future.

- Cybersecurity is one of the major challenges faced by organizations today. As such a dedicated role in executive management with responsibility to manage cybersecurity risks is essential in today's changing climate. Such position will allow to drive consistent policies, procedures and security goals across the organization and be proactive in managing cybersecurity risk and take preemptive action as necessary This will also allow greater accountability and develop a culture of safety within the organization. This position will also help drive better coordination between System Development and System Operations, and integration of security compliance requirements during system design.
- While compliance of PCI-DSS is necessary, only following the minimum requirements is not sufficient. A system is only as strong as its weakest link and hackers are looking for

opportunities to exploit systemic weaknesses or chinks in the armor. Companies should go above and beyond the minimum requirements mandated by PCI-DSS and follow all recommendations, especially when handling critical data such as payment information.

- With top executive management support, companies should develop and nurture a safety culture throughout the depth and breadth of the organization. Some steps to enhance security culture and ensure safety include
    - Identifying and securing the safety critical systems and develop processes and procedures to safeguard them. Periodically review and update this list of safety critical systems.
    - Proper training of employees who are dealing with critical systems within the company and develop best practices to handle and manage such systems.
    - Ensure compliance and enforce safety guidelines without exception. This includes policies for strong passwords and security patches.
    - Separate the safety critical systems from other less critical systems. This requires careful planning during development phase of system design as well as during system integration.
- While adapting to new technologies and systems, always evaluate the security risks involved. Complex systems allow for more opportunities to hackers for breaching and attackers look out for the simplest ways to break into systems.
- Develop a more proactive approach to managing cybersecurity risks. Monitor blogs and forums used by hackers and keep abreast with the latest happenings in cyber-crimes. The types of malware that were used in Target attack were not new and were available on sale on criminal forums much before the attack took place [Dell 2014]. Companies should monitor such sites and look out for new malwares and attack tactics. Then they should evaluate the systems and identify possible avenues that hackers can exploit using these new tools and methods.
- Develop a holistic approach to cybersecurity. Security is more than just following some protocols and developing perimeter defense or following set of procedures. Security is a system property which emerges when different parts of the system work in unison in relation to managing risks and following mandated policies. Every component has a stake in ensuring security of the larger system.

The STAMP/CAST analysis is complete with these list of recommendations. It's evident that the STAMP/CAST analysis and using systems thinking leads to insights which would otherwise not have been visible using other methods of analysis.

11: Comparison of STAMP with Kill Chain

"I never guess. It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts." - Sir Arthur Conan Doyle, Author of Sherlock Holmes

This section compares the recommendations of STAMP on Target cyber-attack with another popular method, Kill Chain Analysis (Table 11.1). The comparison is based on the report submitted by the committee on commerce, science and transportation to the US senate [Kill Chain 2014].

11.1 Comparison Table

#	Recommendation	Kill Chain	STAMP
1	Develop a safety culture	No	Yes
2	Create an executive level role for managing cyber security risks	No	Yes
3	Understand limitations of PCI-DSS and safety standards in general	No	Yes
4	Limit amount of publicly available vendor information	Yes	No
5	Limit the amount of information related to internal system architecture	No	Yes
6	Vendor should have used broadly accepted anti-malware software	Yes	No
7	Vendor Training on phishing attacks and malware	Yes	Yes
8	Target should require two factor authentication	Yes	Yes
9	Follow up on alerts raised by anti intrusion software	Yes	Yes
10	Pay greater attention to industry and government intelligence analysis	Yes	Yes
11	better account management, eliminate unused or default accounts	Yes	Yes
12	Analyze location of credentials users within the system	Yes	Yes
13	Strong firewall between Target's internal systems and Internet	Yes	Yes
14	Whitelisting approved Target's FTP servers used for uploading data	Yes	No*
15	Take action on exfiltration alert	Yes	No*
16	Review system architecture and system design	No	Yes

** indicates that not enough information is provided about the case for STAMP to analyze this aspect. If sufficient details about Target case are obtained (e.g. did it maintain a list of approved FTP servers), STAMP can also provide similar recommendation as Kill Chain*

Table 11.1: Comparison of Kill Chain v/s STAMP Recommendations

STAMP/CAST analysis specifically recommends executive level role for cybersecurity and developing a safety culture (#1 and #2). It also recommends understanding the limits of security protocols like PCI-DSS. While STAMP recommends limiting publicly available information about internal system architecture, it does not view vendor information as being critical (#5). STAMP also does not insist that vendors should have latest malware software. This is largely because vendors are outside the system boundary and it's difficult to exercise control and gather feedback on their practices. STAMP recommends instead securing access to its systems and using dual authentication to further safeguard itself. Finally, STAMP recommends review of system architecture and design and taking a holistic view of security within the organization.

It's evident from the above analysis that STAMP reveals systemic issues which led to the Target cyber-attack. These issues are not captured by Kill Chain Analysis. Also evident from the above discussion and investigation is that STAMP provides several recommendations and insights which are not captured by other popular methods. STAMP can thus be a valuable supplement in understanding and deciphering cybersecurity attacks and help companies such as Target to prevent such attacks from happening in future.

11.2 Recommended Steps and Conclusions

Cyber Threats are getting more severe and hackers more sophisticated. A multi-pronged approach in dealing with cyber-crimes is required and one needs to integrate STAMP with other frameworks and methodologies.

This research builds up upon previous work done for applying STAMP analysis for the TJX case [Cyber Safety CISL, Hamid 2014] in applying a new approach to manage cybersecurity risks. This research based on Systems Thinking and Systems Theory, applies STAMP framework to identify underlying causal factors which led to the Target cyber-attack. Application of STAMP to Target case study as well as to TJX in previous study [Cyber Safety CISL, Hamid 2014] highlighted that STAMP can be effective in analyzing cybersecurity attacks. Insights are revealed which would have been difficult by applying traditional technology focused approaches.

Businesses need to develop expertise in risk identification and management and employ and train sufficient number of security professionals. Information about new attacks or system vulnerabilities may be reported in industry literature or appear in internal system logs. Static security measures against today's Advanced Persistent Threats (APT's) are not sufficient and an in depth and dynamic approach to security is required.

12: Critical Security Controls for Effective Cyber Defense

"You have a right to perform your prescribed duty, but you are not entitled to the fruits of action. Never consider yourself the cause of the results of your activities, and never be attached to not doing your duty." Sri Krishna, Srimad Bhagwad Gita

As is evident, STAMP alone is not sufficient to capture all the insights. To make STAMP analysis more effective, essential security controls have to be in place in the hierarchical control structure.

In 2008, the US federal government along with a consortium of public and private organizations came up with a list of Critical Control based on various cybersecurity lists and guidelines. These controls are published by Center of Internet Security (CIS) in their publication, "Critical Controls for Effective Cyber Defense" [SANS CIS]. The value of these controls is determined by shared knowledge and data and the ability to prevent, alert and respond to cyber-attacks which are all too prevalent today. These list of controls are not just another checklist or things to do but a high priority set of actions that have vast community support network to make them implementable, usable, scalable and be compliant with industry or government security standards [SANS 2014].

12.1 Five Tenets of Effective Cyber Defense System

According to CIS, the five tenets of an effective cyber defense system, as reflected in the critical security controls include [SANS 2014]:

12.1.1 Offence Informs Defense

Use knowledge of attack attacks that have compromised systems and learn from these events to build effective defense for the future. Experience has shown that many of the cyber attackers exploited similar weaknesses in the systems, e.g. credit card payment systems and PCI compliance standard.

12.1.2 Prioritization

Since every organization has limited resources and budgets, invest first in controls which provide greatest benefit in risk reduction and protection against dangerous threats.

12.1.3 Metrics

Another task is to establish common metrics to provide a shared language to IT executives, security specialists and auditors when talking of security risks and threats. This will also lead to effective communication as well as provide the ability to measure effectiveness of the security measures.

12.1.4 Continuous Diagnostics and Mitigation

This cannot be a static activity and security professionals within the organization need to do continuous evaluation and validation of the security measures and to help drive the priority of next steps.

12.1.5 Automation

Lastly, the security controls have to be automated so that organizations can achieve scalable and reliable measurements of the various controls and other metrics.
Based on this report, the 20 Critical Security Controls are listed in Table 12.1 below.

Critical Security Control	Definition
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protections
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account Monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

Table 12.1: List of Critical Security Controls – CIS [SANS 2014]

The details of the critical security controls are provided in the CIS Report [SANS CIS]

12.2 Target Case – Critical Security Controls Violated

As is evident by evaluating this list, implementing these critical security controls at different levels in the hierarchical control structure could have helped prevent Target cyber-attack. For e.g., "Controlled Access Based on the Need to Know" - CSC 14, could have been applied to prevent critical implementation details of virtualization software from being published on internet. The Table 12.2 below maps the Target attack vectors to the Critical Security Controls defined above [SANS 2014]

Target Attack Vectors	Critical Security Control*
Reconnisance	9, 15
Email attack, Malare installed on vendor machines	5, 9
Hacking Vendor Credentials	13, 16
Exploit vendor portal vulnerabilities	3, 6, 20
Infiltration into vendor network	12, 14, 19
Misconfigured systems and vulnerable domain controller	3, 16
Malware installed on POS systems	2, 3, 5, 12
Card data scraped from memory	6, 17
Data removed from POS machines to corporate LAN	3, 13
Data moved to drop locations	17
Failure to respond to FireEye alerts	4, 9, 14, 17, 18, 20
Cards stolen on black market	17

**** The numbers indicate the corresponding Critical Security Controls recommended for each attack vector in Target attack***

Table 12.2: Mapping of Target Attack Vectors to Critical Security Controls [SANS 2014]

13: Applying Cloud Migration Framework to Target

"Behold, the fool saith, "Put not all thine eggs in the one basket" - which is but a matter of saying, "Scatter your money and your attention"; but the wise man saith, "Pull all your eggs in the one basket and - WATCH THAT BASKET." - Mark Twain, Pudd'nhead Wilson

Now having done a comprehensive analysis of the Target breach and identified the causal factors as well as a list of recommendations, we will apply the cloud migration framework to Target and analyze the results. It may be noted that this analysis is a very high level and simplified since we don't have enough knowledge about Target's existing IT structure. For the purpose of this analysis, we will use any typical large company IT infrastructure as a reference.

13.1 Apply the Seven Step Framework

13.1.1 Step One: Identify the Assets for Cloud Deployment

For a typical large retailer like Target, some of the main IT software and data applications would include:

- Payroll Systems
- Supplier and Supply Chain, Procurement
- Finance/Accounting
- Sales and Marketing, Products, Competitive Info
- Communication (email, IM etc.)
- Third Party Vendors, Contractor Billing
- Travel Booking
- Information Systems, Retail Store Systems, POS

These have to be organized into workloads with similar requirements, functionality and security requirements. As an example, all third party billing systems could be classified as "Billing Systems" workload. This is similar to the "Ariba" billing system that Target's contractor Fazio Mechanical used to access its billing systems.

13.1.2 Step Two: Evaluate the Assets for Cloud Deployment

The next step is to evaluate the potential assets for cloud deployment. The company needs to evaluate the security requirements, risk exposure, compliance and other regulatory requirements, performance as well as strategic value of the assets. The assets can be ranked using qualitative and quantitative metrics. Figure 17.1.2 illustrates the qualitative ranking of assets based on their heat map. It can be assumed that a workload such as billing system is low risk application and of less strategic value compared to systems such as supply chain or procurement services. This system is only used by external contractors to bill target for their services and as such doesn't contain any high risk or security information. This workload could be a go and be considered for deployment to cloud.

13.1.3 Step Three: Map the Asset to Potential Deployment Models

After identifying potential workloads for cloud, the next step is to identify the potential deployment model. The company has to evaluate the characteristics and requirements of the application. Such billing systems can have low or medium performance requirements and require moderate security. There is no persuasive need for local caching of data and the goal of the company is to minimize costs for such applications as they don't contribute directly to the bottom line. These requirements are best met by public cloud deployment (Table 3.2). Public cloud offers the right tradeoff between cost, performance and security requirements for such an application.

13.1.4 Step Four: Evaluate Potential Cloud Service Models

The next step in the flow is to select the potential cloud service model. Target is not in the business of software development and one can assume that it's not it strong forte. As such most likely it would refrain from developing its own software billing system and would rather use a software package similar to "Ariba" to manage its billing services. Companies want to generally focus on their key goals and mission (e.g. for Target its retail services) and outsource non critical tasks to external parties. For billing, it needs a plug and play solution and the degree of security control required is not high as it's a non-critical asset. For these reasons, among the different offerings, Software as a Service (SaaS) would be a plausible alternative to use instead of Platform as a Service (PaaS) or Infrastructure as a Service (IaaS).

13.1.5 Step Five: Evaluate Potential Cloud Service Providers

After having identified SaaS as the deployment model, the next step is to identify the CSP. There are a host of CSP's offering billing services software. The company needs to evaluate which one of these best meets its requirements. It should then to a comprehensive TCO analysis and look at different tradeoffs between managing it internally v's the cloud. It should also evaluate the security controls that are necessary for migrating to cloud and develop a high level framework for cloud migration [AWS Cloud].

13.1.6 Step Six: Sketch the Potential Data Flow

The next step is to map the potential data flow. In case of the billing system, the data flow is relatively simple with cloud acting as a mediator between Target and the external vendors. Figure 13.1, illustrates the data flow.

Figure 13.1: Potential Dataflow between Target IT Systems and Vendors for Cloud Deployment of Billing System

Since it's a SaaS application, CSP is responsible for the security and safety of the data and application, however Target still needs to have an Identity Access Management (IAM) system in place.

13.1.7 Step Seven: Making the Final Decision

The final step in the workflow is making the decision. The company needs to do a comprehensive analysis which includes TCO, Return on Investment (ROI) Analysis, Security Evaluation as well as long term migration costs. For security it should evaluate the security metrics and security controls and apply those which it feels are applicable to this application. These must be documented in SLA's using the framework discussed earlier. The company also needs to have a Cloud Migration Framework in place if it decides to deploy systems to cloud [AWS Cloud].

13.2 Conclusion

While cloud migration was applied at a high level for Target case, and several assumptions have been made, this example helps conceptualize the framework and helps in applying the various security metrics and controls discussed earlier. Assuming that migrating the billing system to cloud is feasible and cost effective, it has additionally several advantages for Target.
It helps reduce a potential attack vector. The attackers hacked Fazio's credentials and installed malware to steal its credentials. Cloud providers have better security controls and IAM systems and can potentially disrupt such attack vectors. By migrating less critical systems to cloud, Target can focus on better securing its critical systems such as credit card billing systems.

The reason Target migrated to virtualization was to achieve operational efficiencies and cost effectiveness. To achieve the same objectives Target could also have considered moving its software applications to a virtualized private cloud (VPC) and installed its applications as part of the IaaS service model. Along with the scalability and reliability of cloud, VPC's typically have advanced security features such as security groups and network access control lists [AWS VPC]. Along with that cloud offers better patch management for security updates. Cloud migration could have helped prevent additionally some other attack vectors that the hackers used. While this is not to say that moving to cloud would have prevented the cyber-attack, companies need to also evaluate the security benefits of cloud and analyze if cloud migration can alleviate some of their security threats.

14: Contributions and Future Work

"Better indeed is knowledge than mechanical practice. Better than knowledge is meditation. But better still is surrender of attachment to results, because there follows immediate peace." Bhagavad Gita (c. BC 400, Sanskrit Poem incorporated into the Mahabharata)

14.1 Thesis Contributions

To summarize, this thesis has achieved objectives stated in thesis structure.

In the first phase, it explored the different Cloud Computing Deployment and Service Models. The major Cloud Computing issues were discussed. Various security frameworks and metrics were presented including the major ones from NIST and CSA. The critical areas of focus for cloud security were presented. Then, the various critical cloud security threats were mapped to cloud security domains and different service platforms. Some of the major security benefits were also discussed. The cybersecurity metrics defined by CIS were presented cloud specific security metrics were explored. NIST cybersecurity controls as well as security controls specific to cloud as developed by CSA were presented. Service level Agreement framework for cloud was discussed and SLA's for different cloud service models were touched upon. Then a high level cloud migration framework strategy and framework was presented. This framework can be used by CIO/CSO's of companies who are evaluating the decision to migrate to cloud.

In the second phase, Systems Thinking and Systems Theory was applied to Target security breach. The need for Systems Thinking approach to cybersecurity and developing a holistic approach in solving such problems was highlighted. Specifically, the STAMP/CAST framework was applied to the data breach. Based on the STAMP/CAST analysis, key recommendations were presented that companies like Target can use to manage cybersecurity risks and prevent such similar attacks in the future. New insights were discovered when applying STAMP/CAST to the Target case and several insights were favorable when compared to traditional Kill Chain method.

Finally, in the third phase, the cloud migration framework discussed in phase one was applied to Target. A case was made that in certain scenarios, moving the less critical applications to cloud and utilizing the security benefits of cloud can actually reduce the threat vectors and security exposures and bring IT systems from a higher risk state to lower risk state.

For this thesis, only reports and publications that were available in the public domain were utilized. So there was limited information available with regards to Target's actual IT structure and organizational details, as well as the actual security infrastructure and controls they had in place before the attack. Cybersecurity is a critical and sensitive issue for organizations and in general it's hard to get detailed information about its actual implementation within the company. This thesis and the analysis was limited by the amount and accuracy of the information available from public sources.

14.2 Future Work

Many systems engineering decisions are complex because they include multiple stakeholders often with competing needs, multiple objectives, many unknowns and alternatives, and there is lot of uncertainty. The decision to migrate to cloud shares many characteristics of a complex systems engineering decision. Enterprises need to balance risks and opportunities over the entire system life cycle. Systems engineering decision management processes and framework are ideally suited for these kind of problems. An attempt was made to quantify several risk and security metrics and apply a high level framework to cloud migration. This framework was applied to Target as a use case, after using the insights and recommendations based on STAMP analysis. While this thesis accomplished set objectives, it also presents an opportunity to focus on several issues that are still unresolved. Some of these are listed below:

- Apply the System Theoretic Process Analysis (STPA) approach to identify system vulnerability prior to an attack.
- Apply STAMP/CAST/STPA to instill a culture of security (socio technical context)?
- Integrate STAMP with other widely used Cybersecurity Controls.
- Develop applicable quantitative security and risk metrics for Cloud.
- Develop several use cases of Cloud Migration and run through the model to validate it (using actual company data).
- Implement Trade space (MATE) decision analysis for a real world example. Trade studies aim to maximize stakeholder value and system utility by balancing various system objectives to provide the optimum solution, so this could be interesting area of research.
- In general, what are the scenarios in which migrating to cloud mitigate cyber-attacks such as Target?

15: Bibliography

[Aissa 2010]. Ben Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A., 2010. Quantifying security threats and their potential impacts: a case study. Innovation in Systems and Software Engineering: A NASA Journal 6, 269–281.

[Aorato 2014]. "The Untold Story of the Target Attack Step by Step" Aorato Labs August 2014

[Arash Madnick]. A. Nourian, S. Madnick. 2016. "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet".

[AWS 2010]. "Migrating Your Existing Applications to the AWS Cloud", Amazon Web Services publication, Jinesh Varia, October 2010

[AWS 2011]. Architecting for the Cloud: Best Practices, Jinesh Varia, January 2011. Referenced from https://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

[AWS DirectConnect]. Referenced from https://aws.amazon.com/directconnect/

[AWS EC2]. Referenced from https://aws.amazon.com/ec2/

[AWS VPC]. Referenced from https://aws.amazon.com/vpc/

[Baldwin 2014]. Baldwin, H. 2014. The other shoe drops for Target's CIO. Retrieved from Forbes: http://www.forbes.com/sites/howardbaldwin/2014/03/11/the-other-shoedrops-for-targets-cio/

[Black 2009]. Black, P.E., Scarfone, K., Souppaya, M., 2009. Cybersecurity Metrics and Measures. Wiley Handbook of Science and Technology for Homeland Security.

[Brunette 2009]. Security guidance for critical areas of focus in cloud computing V 1.2. Cloud Security Alliance, Brunette, G., Mogull, R., 2009.

[CAMM 2011]. Common Assurance Maturity Model, Raj Samani. Referenced from http://www.fstech.co.uk/fst/FSTech_Conference_2011/Common_Assurance_Maturity_Model_Raj_Samani.pdf

[Chow 2009]. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuok, R., Molina, J., 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: ACM Workshop on Cloud Computing Security (CCSW).

[CIS 2010]. The CIS Security Metrics, Nov 1st 2010. Referenced from https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

[Cloudbolt 2016]. CloudBolt Blog, 2016, Bernard Sanders. Referenced from http://get.cloudbolt.io/blog

[CMU 2010]. J. Cebula, L. Young, Dec 2010. A Taxonomy of Operational Cybersecurity Risks. Referenced from http://www.sei.cmu.edu/reports/10tn028.pdf

[COBIT 2013]. An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model, Shengnan Zhang, Hans Le Fever, Nov 2013

[COBIT]. Referenced from http://www.isaca.org/cobit/pages/default.aspx

[COSO 2013]. Crowe Horwath, Warren Chan, Eugene Leung, Heidi Pili, Enterprise Risk Management for Cloud Computing, Committee of Sponsoring Organizations of the Treadway Commission, June 2013

[CSA 2009]. Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance Dec 2009.

[CSA 2010]. Top Threats to Cloud Computing V1.0, March 2010

[CSA 2011]. Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance V3.0, 2011. Referenced from https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

[CSA 2016]. The Treacherous 12, Cloud Computing Top Threats in 2016. Referenced from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[CSA CCM]. Referenced from https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[Cyber Safety CISL]. "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cybersecurity Risks", Hamid Salim, Stuart Madnick, Working Paper CISL# 2014-12. Referenced from http://web.mit.edu/smadnick/www/wp/2014-12.pdf

[Dell 2014]. "Inside a Targeted Point-of-Sale Data Breach", Keith Jarvis and Jason Milletary Dell SecureWorks Counter Threat Unit Threat Intelligence, 24th Jan 2014

[Elgin 2014]. Elgin, B. 2014, March 13. Missed alarms and 40 million stolen credit card numbers: How target blew It. Retrieved from Bloomberg Businessweek: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

[ENISA 2009]. "Cloud Computing Benefits, Risks and recommendations for Information Security", ENISA Nov 2009. Referenced from https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[FTA]. Referenced from https://en.wikipedia.org/wiki/Fault_tree_analysis

[Gomzin 2014]. Gomzin, S. (2014). Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions. Indianapolis, IA: Wiley.

[Gonsalves 2014]. Gonsalves, A., 2014, May 5. Target CEO resignation highlights cost of security blunders. Retrieved from CSO: http://www.csoonline.com/article/2151381/cyberattacks-espionage/target-ceo-resignation-highlights-cost-of-security-blunders.html

[Hamid 2014]. Hamid Salim, 2014. "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks". Master's Thesis. Engineering Systems Division. Massachusetts Institute of Technology. 2014. Referenced from https://dspace.mit.edu/handle/1721.1/90804

[iSight 2014]. iSight Partners. 2014. KAPTOXA Point of sale compromise. Retrieved from Security Current: www.securitycurrent.com/.../KAPTOXA-Point-of-Sale-Compromise.pdf

[ISO]. Referenced from https://en.wikipedia.org/wiki/International_Organization_for_Standardization#Criticism

[Jonsson 2011]. Jonsson, E., Pirzadeh, L, 2011. A framework for security metrics based on operational system attributes. In: International Workshop on Security Measurements and Metrics – MetriSec2011, Banff, Alberta, Canada.

[KC 2014]. Referenced from http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

[KC CSO]. Referenced from http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

[Kill Chain 2014]. "A kill Chain analysis of the target 2013 data Breach", Majority Staff Report for Chairman Rockefeller March 26, 2014 to US Senate Committee on Commerce, Science and Transportation

[Krebs 2013]. Krebs, B. 2013c, December 12. Cards stolen in Target breach flood underground markets. Retrieved from Krebs on Security: http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-floodunderground-markets/

[Krebs 2014]. Brian Krebs, *New Clues in the Target Breach*, KrebsOnSecurity (Jan. 29, 2014) Referenced from http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach

[Krebs 2015]. Referenced from http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

[Latifa 2013]. Latifa Ben, Arfa Rabai, Mouna Jouini, Anis Ben Aissa , Ali Mili. A cybersecurity model in cloud computing environments, Journal of King Saud University – Computer and Information Sciences (2013) 25, 63–75

[Leveson 2011]. N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety,* Cambridge, MA: MIT Press, 2011. Referenced from https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262016629_Engineering_a_Safer_World.pdf

[Leveson CAST]. N. G. Leveson, "Analyzing Accidents and Incidents (CAST)," in *Engineering a Safer World: Systems Thinking Applied to Safety,* Cambridge, The MIT Press, 2011, pp. 350-390.

[Leveson NASA]. Technical and Managerial Factors in the NASA Challenger and Columbia Losses: Looking Forward to the Future by Nancy Leveson, in Handelsman and Kleinman (editors), Controversies in Science and Technology, University of Wisconsin Press, 2007.

[Leveson STAMP 2004]. A New Accident Model for Engineering Safer Systems, April 2004. Referenced from http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[Leveson STPA]. *N.* G. Leveson, An STPA Primer, August 2013. Referenced from http://sunnyday.mit.edu/STPA-Primer-v0.pdf

[Mandiant 2014]. Mandiant, 2014. M Trends: beyond the breach. Alexandria, Mandiant.

[Luna 2011]. Jesus Luna, Hamza Ghani, Daniel Germanus and Neeraj Suri, A security metrics framework for the cloud, Department of Computer Science, Technische Universit¨at Darmstadt, Hochschulstr. 10, 64289 Darmstadt, Germany, Jan 2011

[Mayer 2009]. Mayer, N., 2009. Model-Based Management of Information System Security Risk. PhD Thesis.

[Mccombs]. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[McKinsey 2011]. "Getting ahead in the cloud", McKinsey Report 2011, Kreg Nichols and Kara Sprague

[Microsoft 2011]. Referenced from https://redmondmag.com/articles/2011/03/21/microsoft-touts-server-virtualization-for-target.aspx

[MIT MATE]. Referenced from http://seari.mit.edu/mate.php

[NIST – ITL]. Referenced from http://www.nist.gov/itl/cloud/

[NIST 2014]. Framework for Improving Critical Infrastructure Cybersecurity, NIST, Feb 2014 Referenced from http://www.nist.gov/cyberframework/upload/cybersecurity-framework 021214.pdf

[NIST 2015]. Referenced from http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf

[NIST 2016]. Cybersecurity Framework Workshop, April 2016 Referenced from http://www.nist.gov/itl/acd/cybersecurity-framework-workshop-2016.cfm

[NIST SLA]. Cloud Computing Service Metric Description, NIST Cloud Computing Reference Architecture and Taxonomy Working Group, Special Report 2015. Referenced from http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf

[NIST, 2011]. The NIST Definition of Cloud Computing, September 2011, Peter Mell, Timothy Grance, Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[NIST-Metrics]. Recommended Security Controls for Federal Information Systems, NIST. Referenced from http://infohost.nmt.edu/~sfs/Regs/sp800-53.pdf

[OCTAVE CMU]. Cyber Risk and Relience Management, CMU. Referenced from http://www.cert.org/resilience/products-services/octave/

[Pat SDM]. Pat Hale. 2008. "Systems Thinking Comes of Age". Referenced from https://sdm.mit.edu/conf08/presentations/pat_hale.pdf

[PCI]. Referenced from https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

[Pereira STAMP] "A System-Theoretic Hazard Analysis Methodology for a Non-Advocate Safety Assessment of the Ballistic Missile Defense System, June 2006

[Poulin 2014]. Poulin, C. What retailers need to learn from the Target breach to protect against similar attacks. Retrieved from Security Intelligence: http://securityintelligence.com/target-breach-protect-against-similar-attacksretailers/#.U8sthsLn-pp

[Ross 2005]. Referenced from http://web.mit.edu/adamross/www/Ross_INCOSE05.pdf

[SANS 2014]. Case Study: Critical Controls that Could Have Prevented Target Breach, Teri Radichel, SANS Institute, August 5th 2014

[SANS CIS]. Referenced from https://www.sans.org/critical-security-controls

[SANS SLA]. Proposal for standard Cloud Computing Security SLAs - Key Metrics for Safeguarding Confidential Data in the Cloud, SANS Institute, Michael Hoehl, Manuel Humberto Santander Pelaez

[SEI CMU]. Referenced from http://www.sei.cmu.edu/sos/research/cloudcomputing/cloudbarriers.cfm

[Target 2011]. Microsoft Virtualization: Customer Solution Case Study. Referenced from http://download.microsoft.com/download/3/A/D/3AD464EA-F2B4-4E62-B11F-14E37727557C/Target_Hyper-V_CS.PDF.

[Target 2014]. Target, *Target Provides Update on Data Breach and Financial Performance* (Jan. 10, 2014) (online at http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance).

[TechTarget Cloud]. Referenced from: http://searchcloudcomputing.techtarget.com/feature/Cloud-data-security-comes-at-a-cost

[TechTarget]. "Getting Started with Cloud Storage", TechTarget Report. Referenced from http://cdn.ttgtmedia.com/CascadingTargetedDownloads/downloads/Cloud-storage%20definition.pdf

[Young 2014]. W. Young, N. Leveson. 2014. "An Integrated Approach to Safety and Security based on Systems Theory," Commun. ACM, vol. 57, no. 2, pp. 31–35, 2014.

[Weiss 2015]. "The Target and Other Financial Data Breaches: Frequently Asked Questions", N. Eric Weiss, Rena S. Miller, Feb 4th 2015

[Wiki EaaS]. Referenced from https://simple.wikipedia.org/wiki/Everything_as_a_service

[Wikipedia – Cloud Issues]. In Wikipedia, the free encyclopedia. Referenced from https://en.wikipedia.org/wiki/Cloud_computing_issues

[Wikipedia – Cloud]. In Wikipedia, the free encyclopedia. Referenced from https://en.wikipedia.org/wiki/Cloud_computing

[Zdnet 2015]. Referenced from http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/