PRICE®

COST ESTIMATION SOLUTIONS

Estimate with Confidence™



Cybersecurity in the Cloud

PSM 2018, September 13,2018

Introduction

Cloud Computing is defined by National Institute of Standards and Technology (NIST) …

"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 release with minimal management effort or service provider interaction"

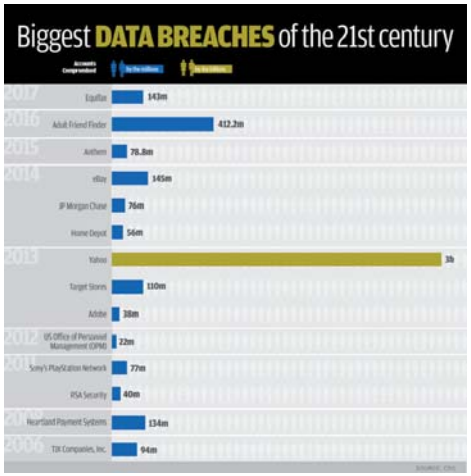
Hybrid Cloud Computing or Hybrid IT is defined as…

"a cloud computing environment which uses a mix of on-premises, private cloud, and third party public cloud services with orchestration between the platforms"

According to a Forbes report from April 2017, hybrid cloud adoption grew 3x in the last year from 19% to 57%

Cloud Security Breaches

- **Anthem Inc.**
  - Second biggest healthcare insurer in the nation
  - Breach affected 10's of millions of customers
  - Hackers smuggled data out of cloud-based file sharing service
- **DropBox**
  - Hackers tapped into 68 million user accounts – emails and passwords
  - Stolen credentials to the dark web
- **Code Spaces**
  - Cloud based software development environment
  - Hackers compromised the site and demanded a ransom
  - Hackers then systematically started deleting customers coding projects
  - Put company completely out of business
- **Home Depot**
  - An attack occurred at the point-of-sales terminals at the self checkout lanes
  - This went on for months before it was detected
  - 56 Million credit card numbers were stolen

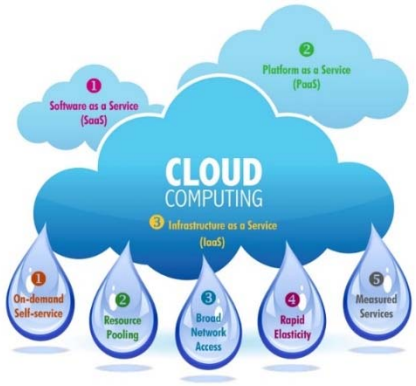


Typical Security Breaches

- Insider accidental act (deletion of data e.g.)
- Cyber Criminal DDoS (Distributed Denial of Service)
- Fraud or extortion attempts
- Insider malicious act(theft or destruction)
- Ransomware outbreak
- Credit care or other personal information data breach
- Extended internet outage
- Theft or loss of hard drive, mobile device, USB device containing sensitive data

Cloud Computing

Cloud Computing Overview



According to NIST, cloud computing delivers five essential characteristics

- On demand self service – required IT resources are available when and where they are needed
- Broad network access – all one needs is a browser and a network connection to get to their applications and data
- Resource pooling – the location of the data centers is irrelevant – allowing cloud providers to pick locations where real estate and power are affordable
- Rapid elasticity – through virtualization and distributed processing the offerings expand and collapse based on the users requirements for resources
- Measured service – infrastructure is in place to monitor and measure service deliveries – with automatic correction and optimization

Cloud Computing Platforms

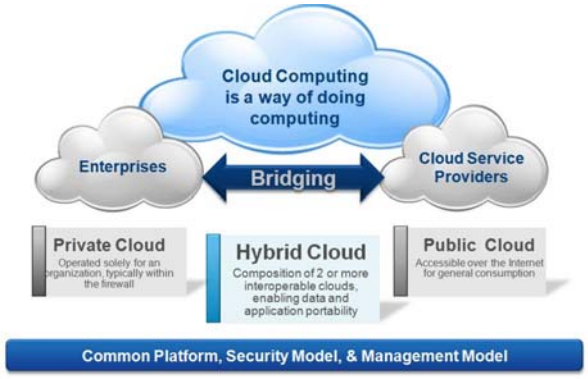
- **Public Cloud**
  - Available to any user of the Internet willing to meet the terms and condition of the cloud service provider.
  - Key characteristic of public cloud computing is multi-tenancy
- **Private Cloud**
  - Cloud computing infrastructure and technologies are maintained and operated for a single organization, department or agency
  - Private cloud could be housed on premise or remotely
  - Could be run internal resources or a cloud computing provider
  - Private cloud applications service a single customer
- **Hybrid cloud**
  - Intermingling of private cloud, public cloud and on premise resources
  - Organizations take advantage of public cloud where it makes sense and use private or on-premises solutions where data and applications are sensitive

Hybrid Cloud/Hybrid IT Environment

- **Joins together public cloud, private cloud and on-premises solutions to deliver a single workload or application**
- **Encrypted connections between the solutions**
- **Technology that makes data portable among the solutions**
- **Allows organizations to leverage benefits of cloud computing while defending the integrity of sensitive data and applications**
- **Workload options include**
  - Public cloud
    - Infrastructure as a Service
    - Software as a Service
  - Hosted private cloud
  - On-premises private cloud
  - On-premises infrastructure in enterprise data center
  - Off-premises data center facility

Benefits of Hybrid Cloud Solutions

- **Security**
  - Store sensitive stuff in private cloud or on-premises but utilize public cloud resources to process data
- **Availability**
  - Organizations can prevent downtime by keeping certain functions accessible and on-site.
- **Performance**
  - Functions that require high speed may not make sense as public cloud applications. High volume and real time applications may require private or on-premises availability
- **Cost efficiency**
  - Using the public cloud where it makes sense will offer cost savings (costs spread among many customers)



Hybrid Cloud Security Challenges and Mitigations

Hybrid Cloud Security Challenges & Mitigation Strategies

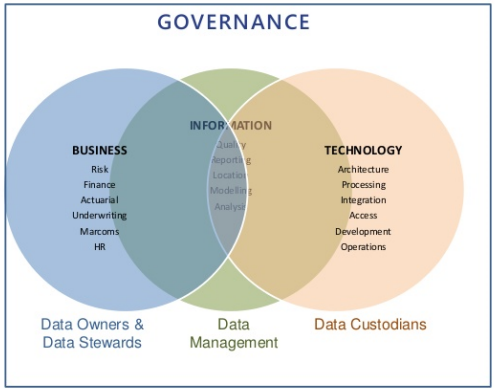
- **Compliance**
  - Compliance refers to industry or government wide regulations and rules that govern how data is managed
  - With hybrid solutions data is moving from provider to provider or from on-premises to public cloud
  - Compliance requirements need to be recognized and enforced by all parties handling the data
  - Poor compliance could result in compromised data
- **Mitigation**
  - Ensure cloud provider can pass third party audits as part of a standard check for required compliance
  - Make sure all cloud solutions are coordinated in their exchange of data
  - Make sure that all cloud solutions meet industry standards for data security
  - Ensure that your organization can also pass a third party audit with respect to required compliance

Hybrid Cloud Security Challenges & Mitigation Strategies

- **Poor Service Level Agreements (SLAs)**
  - Service Level Agreement is a contract between a service provid and the end user. It defines the level of service expected of the provider and the consequences if that level is not achieved
  - Cloud consumers need to understand the SLAs with their cloud providers
  - Cloud consumers need to understand what the SLA does not cover and where their responsibilities take over.
- **Mitigation**
  - Access permissions and protections must be well clarified in the SLA
  - Security measures must be well defined
  - SLA should clearly and conclusively state where responsibility for security is the providers and where it is the consumers
  - Make sure compliance requirements are clearly spelled out
  - Read the fine print!

Hybrid Cloud Security Challenges & Mitigation Strategies

- **Lack Data Ownership/Poor Governance**
  - Once data is deployed in the cloud, enterprises can lose some ability to govern their data
  - Cloud consumers need to be aware of what security levels are available from their cloud providers
  - Cloud consumers need to understand
    - Who owns the data
    - What policies govern the data
    - How are policies enforced



- **Mitigation**
  - Every asset must have an owner who is responsible for
    - Least privilege (Principle of least privilege requires that in a particular abstraction layer of a computing environment every module must be able to access only the information and resources that are necessary for its legitimate purpose)
    - Segregation of duties over the asset
  - Governance policies should be maintained and updated as cloud deployment is considered and implemented

Hybrid Cloud Security Challenges & Mitigation Strategies

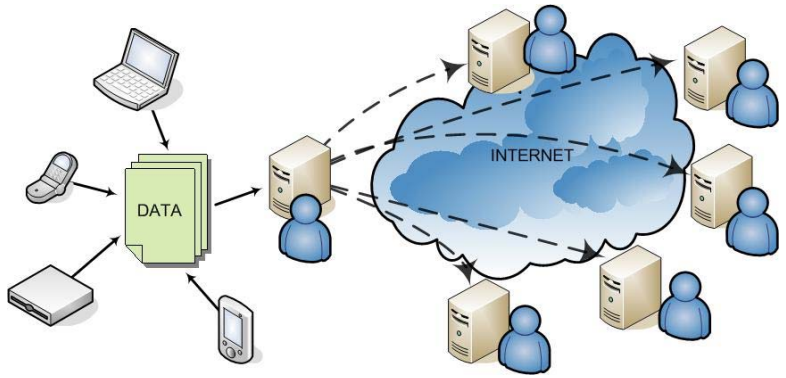
- **Lack of Encryption**
  - Encryption is the process of converting data into some sort of code, mostly used to prevent unauthorized access
  - Data encryption is necessary whenever data is transmitted
  - It is also important that sensitive data be encrypted at rest when it is stored in the cloud
  - Encryption should be an important part of any compliance strategy
- **Mitigation**
  - Employ a viable VPN
  - Use a reliable proxy server
  - Encrypt all transmissions using SSL/TLS to manage server authentication (Secure Sockets Layer/Transport Layer Security)

Hybrid Cloud Security Challenges & Mitigation Strategies

- **Data leakage**
  - Data leakage is the unauthorized transfer of classified information from a computer or data center to the outside world
  - Clearly a hybrid cloud solution with data moving from point to point can be more susceptible to data leakage
  - Inadequate security controls on the part of the cloud provider can compromise data. This can be especially true in environments where BYOD is practiced by employees
  - It's important to stay aware of what's happening with your data and where it is going
- **Mitigation**
  - Make sure provider has coverage for data leakage – SLA should indicate consequences of data loss
  - Security management plans should indicate counter measures for infrastructure malfunctions, security breaches and software defects leading to vulnerabilities

Hybrid Cloud Security Challenges & Mitigation Strategies

- **Poor Data Redundancy**
  - Data redundancy simply means that the same piece of data is stored in more than one place.
  - Data critical to an organization should be in more than one place
- **Mitigation**
  - Consumers should take advantage of multiple data centers from providers
  - Look for private or public cloud vendors that address redundancy as part of their business model

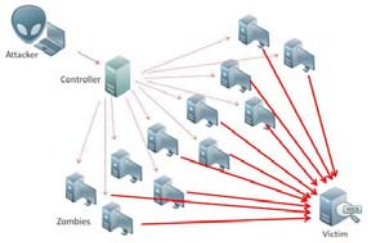


Hybrid Cloud Security Challenges & Mitigation Strategies

- **Weak Security Management**
  - Security management involves an examination of an organizations assets followed by the development, documentation and execution of policies and procedures for protecting those assets
  - These procedures should address
    - Authentication of users
    - Identity management
    - Authorization procedures

- **Mitigation**
  - Make sure that controls are replicated for all of the cloud solutions
  - Make sure that security data is synchronized
  - Use an identity management system that works with the cloud solutions you deploy
  - Consider multi-factor authentication

Hybrid Cloud Security Challenges & Mitigation Strategies



- **Denial of Service (DoS)/Distributed Denial of Service (DDoS)**
  - A DoS attack is a cyber-attack where a malicious entity attempts to make a machine or resource unavailable to its intended users by disrupting services of host connected to the Internet. Disruption is generally through weakness in shared resources such as CPU, RAM, disk space or network.
  - A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system. Disruption is through high volume incursions distributed from multiple sources.
- **Mitigation**
  - Flow analysis may help in identifying symptom of an attack
  - Employ a DoS/DDoS Protection Services such as Arbor Network's APS, Radware's DefensePro, or Fortinet's FortiDDoS
  - Use a Content Delivery Network (CDN) which will provide protection from large surges in traffic

Hybrid Cloud Security Challenges & Mitigation Strategies

- **Disgruntled/Malicious/Sloppy Employees**
  - Among 874 incidents reported to the Ponemon Institute for it 2016 Cost of Data Breach Study…
    - 568 were caused by employee or contractor negligence
    - 191 were by malicious employees or criminals
  - It is not enough for an organization to have policies and procedures in place, there needs to be assurance that those policies and procedures are being adhered to and executed faithfully
- **Mitigation**
  - Track employee network activities
  - Create an insider threat program
  - Make sure access to sensitive data is controlled on a as-needed basis
  - Vigilant execution of security management policy
  - Apply a top down/ bottoms up practice of being aware of what's going on with employees
  - Enact and execute strong password policies

Cybersecurity Measures, Metrics and Controls

CyberSecurity Measures and Metrics

- Organizations need to invest in proactive controls to ensure that:
  - Attacks don't occur
  - If attacks occurred they are identified and corrected quickly
- According to Gartner in 2017 organization's spent 5.6% of their annual IT Budget on security and risk management
- The questions that arise are:
  - Are these the right investments?
  - Did these investments mitigate risk of breaches?
  - If there were breaches, were they detected quickly so that cost of breach was mitigated?
- In order to answer these questions organizations must define measures to assess the effectiveness of their controls

Cybersecurity Measures and Metrics

The Center for Internet Security (CIS) – a 501c3 non-profit whose mission is to identify, develop, promote and sustain best practices for cyber security has developed a comprehensive set of proposed metrics

Category	Metrics
Incident Management	Cost of Incidents
	Mean Cost of Incidents
	Medan Incident Recovery Costs
	Mean Time to Incident Recovery
	Number of Incidents
	Mean Time Between Security Incidents
Vulnerability Management	Vulnerability Scanning Coverage
	Percent of Systems with No Known Vulnerabilities
	Mean Time to Mitigate Vulnerabilities
	Number of Known Vulnerabilities
	Mean Cost to Mitigate Vulnerabilities
Patch Management	Patch Policy Compliance
	Patch Management Coverage
	Mean Time to Patch
	Mean Cost to Patch
Configuration Management	Percent of Configuration Compliance
	Configuration Management Coverage
	Current Anti-Malware Compliance
Change Management	Mean Time to Complete Change
	Percent of Changes with Security Review
	Percent of Changes with Security Exceptions
Application Security	Number of Applications
	percent of Critical Applications
	Risk Assessment Coverage
	Security Testing Coverage
Financial Metrics	IT Security Spending as Percent of IT Budget
	IT Security Budget Allocation

Cybersecurity Measures and Metrics

CIS Created the following cybersecurity scorecard to offer a minimum set of metrics to start with

Scorecard Area	Action	Required Metrics
Impact	Report on security incidents and their impact on the organization.	1. Number of Incidents 2. Cost of Incidents
Performance by Function: Outcomes	Report the outcome of business functions' Configuration Management, Patch Management and Vulnerability Management.	3. Configuration Policy Compliance (using CIS benchmarks) 4. Patch Policy Compliance (using current patch level) 5. Percent of Systems with No Known Severe Vulnerabilities (using CVSS base scores)
Performance by Function: Scope	Report the scope of business functions and the scope of outcome metrics for those functions.	6. Configuration Management Coverage 7. Patch Management Coverage 8. Vulnerability Scanning Coverage
Financial Metrics	Report on the allocation and efficiency of security spending	9. IT Security Spending as Percent of IT Budget 10. IT Security Budget Allocation

DOD Cybersecurity Scorecard

- **Part of the Cybersecurity Discipline Implementation Plan - 2016**
- **Primary goal is to have organizations across the Department go back to Cyber Basics**
- **Four key areas the plan focuses**
  - Ensuring Strong Authentication – how do users log into devices and systems; authentication of accountability of users actions
  - Hardening Devices – Keeping devices properly configured and updated in a timely fashion
  - Reducing the Attack Surface – sensible management of what systems connect to the public internet (cloud) and other external systems
  - Detecting and Responding to Potential Intrusions – rapid identification, quick response, improved defenses
- **Organizations report progress via the DOD CyberSecurity Scorecard**

NIST Security Controls

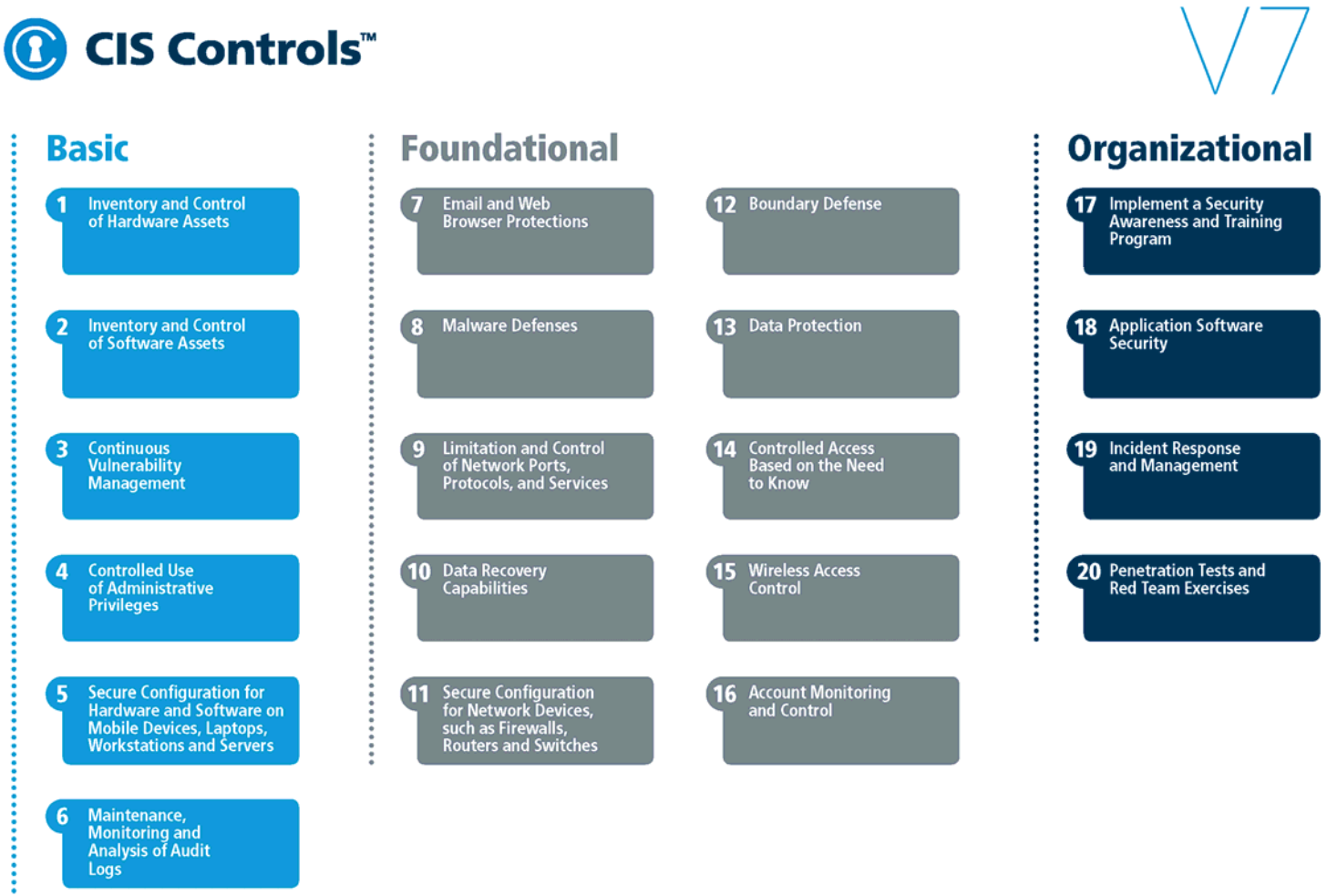
- **NIST 800-53 presents a catalog of security controls for federal information systems and organizations.**
- **The document provides extensive guidance on what they mean and how organizations can select and implement**

Class	Family
Technical	Access Control
	Audit and Accountabiliy
	Identification and Authentication
	System and Communication Protection
Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Physical and Environmental Protection
	Personnel Security
	System and Information Integrity
Management	Security Assessment and Authorization
	Planning
	Risk Assessment
	System and Services Acquisition
	Program Management

CIS Cybersecurity Controls

- **CIS has also developed a set of Controls that organizations should consider employing in total or in part depending on their exposure and budget. These are provided in three categories:**
  - **Basic – Necessary Cyber Hygiene – things all organizations should be on top of**
  - **Foundational – Necessary to protect, identify and correct**
  - **Organizational – Less technical but just as important – making sure the organization as a whole embraces best practices around cybersecurity**

CIS Recommended Controls



Wrap Up

Wrap Up

- Hybrid cloud solutions are excellent for maximizing the value an organization can get out of cloud technology
- These solutions can be very secure but it requires vigilance, common sense and attention to detail from the consumer
- Addressing cybersecurity issues – whether you are in the cloud, on the ground or somewhere in between - is a must for all organizations large and small
- Understanding the risks and understanding how to measure around those risks is important for organizations to understand how best to spend cybersecurity related budget