Microsoft

No Country for Old Security

Compliance in the Cloud

Joel Sloss, CDSA Board of Directors

May 2017

Emerging Threats

- Specific/sequential targeting
- Effective reconnaissance
- Practiced tool usage
- Sophisticated planning
- Social engineering
- Advanced & persistent

"FUNDAMENTALLY, IF SOMEBODY WANTS TO GET IN, THEY'RE GETTING IN...ACCEPT THAT.

WHAT WE TELL CLIENTS IS:
NUMBER ONE, YOU'RE IN THE FIGHT, WHETHER YOU THOUGHT YOU WERE OR NOT. NUMBER TWO,

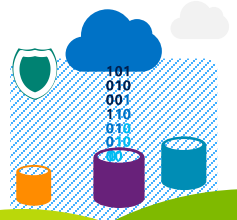
YOU ALMOST CERTAINLY ARE PENETRATED."

Michael Hayden
Former Director of NSA & CIA

Understanding Threats in New Media

File Not Found

- Motivated by economic gain, voyeurism, political gamesmanship
  - Data tampering, theft, loss
  - Service disruption / destruction
  - Competitive advantage
- Multiple attack vectors
  - In-transit: on the wire, portable media / devices
  - At-rest: in storage / archive, on workstations
  - In-use: at the source, on the capture device, in a service / application
- Multiple attack types
  - Admin breach / insider threat
  - Malware
  - And the list goes on …



Trusted Cloud Principles

Security and Compliance Requirements for Media

WHAT

- Regulatory demands
- Protect data
- Isolate workloads
- Control access
- Ensure availability
- Manage risk
- Block threats

Trust

HOW

- Encryption
- VLAN / firewalls
- Physical security
- Redundancy
- Policies / processes
- Training
- Patching

Cloud Compliance – Distributed Accountability

Customer
Provider

Responsibility	On-Premises (as a Service)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Data Classification and Ownership	Customer	Customer	Customer	Customer
Client / Endpoint Protection	Customer	Customer	Customer	Customer
Identity and Access Management	Customer	Customer	Customer / Provider	Customer / Provider
Application-Level Controls	Customer	Customer	Customer / Provider	Provider
Network-Level Controls	Customer	Customer	Customer / Provider	Provider
Host Security	Customer	Provider	Provider	Provider
Physical Security	Customer	Provider	Provider	Provider

Security Domains in Media and Entertainment

Standards and Guidelines

- Cloud Controls Matrix v3.0.1
- Content Protection Standard
- Cloud & Application Security Guidelines
- Federation Against Copyright Theft

+ Relevant Frameworks

Here's an over-simplification: Audit 101

Compliance Objectives

What are you certifying?

- Environment
- Solution
- Application
- Domains
- Scope

Understand Requirements

Are you ready to RoC?

- Capabilities
- Processes
- Policies
- Mechanisms
- Technologies

Identify Responsibilities

What do you own?

- Service provider accountabilities
- On-premises activities
- IaaS/PaaS/SaaS separation

Execute Controls

Do you have what it takes?

- Evidence and artifacts
- Logs and records
- Standard operating procedures

Mapping Requirements to Responsibilities

Subset of critical controls and a common framework

CSA CCM v3.0.1	Your Action
Application Security	Patching, SDL, input validation, data classification
Business Continuity	Fault-tolerant design, backup, testing
Change Control	Monitoring, alerting, reporting
Datacenter Security	None
Encryption Management	Key management, selection, policies
Risk Management	Anti-malware, DDOS/IDS protection
Identity / Access Mgmt	Passwords, multi-factor auth, RBAC
Virtualization Security	Firewalls, network policies
Incident Management	IR Plan, testing, post-breach forensics
Threat Management	Prevent and Assume breach

- Also applies to:
  - CDSA Content Protection & Security Standard
  - MPAA Application and Cloud Security Guidelines
  - FACT (ISO 27001)
- Mapping will be similar

Actions to Capabilities – Continuous Compliance

Things you need in Digital Media and Entertainment

Transfer risk to the cloud

Maintain data governance

Leverage scale and investments

- Dynamic encryption and transcoding
- Secure storage and workflow
- Identity Management, Multi-Factor Authentication, Roles-Based Access Control
- License management / enforcement across platforms
- Content protection throughout lifecycle
- Isolated networking
- Streaming / CDN services
- Security monitoring, logging, and reporting

How? Red Team | Blue Team

Prevent Breach

- Threat model
- Code review
- Security testing
- Security development lifecycle

Assume Breach

- War game exercises
- Central security monitors
- Live site penetration test

Assume breach identifies & addresses significant gaps:

- **Detect attack & penetration**
- **Respond to attack & penetration**
- **Recover from data leakage or tampering**

Scope **ongoing live site** testing of security response plans to drastically improve **Mean Time To Detection & Recovery**

Reduce exposure to **internal attack** (once inside, attackers have broad access)

Periodic environment **post breach assessment & clean state**

References and Further Reading

- CSA CCM
  - https://cloudsecurityalliance.org/group/cloud-controls-matrix/
- CDSA
  - http://www.cdsaonline.org/
- MPAA
  - http://www.mpaa.org/content-security-program/
- Microsoft Enterprise Red Teaming
  - http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf
- Security Development Lifecycle
  - https://www.microsoft.com/en-us/sdl/default.aspx

Thank You! (jsloss@microsoft.com)

QUESTIONS?