Cloud Fails: How to Avoid Them

Larry Swonke  Azure Solutions Director
Carlos Patiño  Azure Consultant
‘Tis the Season...
Fail #1  Netflix Xmas Outage of 2012

Error
There is a problem connecting to Netflix. Please try again later.

Netflix US 📺
@netflix

We're sorry for the Christmas Eve outage. Terrible timing! Engineers are working on it now. Stay tuned to @Netflixhelps for updates.
How to Fail at Cloud

• Learn about developing a successful cloud practice
• Highlight notorious and not so notorious cloud outages
• Deconstruct failure, detail RCA
• Derive lessons learned, how to Detect and Prevent

*Some names have been changed to protect the not so innocent*
Cloud Management Practice Areas

Financial Mgmt.
- Metering
- Invoicing
- Cost Allocation
- Chargeback
- Forecasting

Self Service
- User Portal
- Admin Portal
- Reporting
- Service Catalog

Brokerage
- Aggregation
- Integration
- Intermediation

Resource Mgmt.
- Tagging
- Configuration Management
- Performance Optimization
- De/Provisioning
- Cost Optimization
- Migration

Service Mgmt.
- Incident Management
- Network Operations
- Service Level
- Monitoring

Security
- Security Management
- Security Operations
- Resource Security
- Data Security

Governance
- Compliance
- Policy
- Roles
- Risk Management

Strategy
- Business & Technical Alignment
- Cloud Maturity Improvement
- Monthly Workshops
- Feature Adaptation
- Living Roadmap
- Weekly Briefing

Catapult

Microsoft Partner

2019 Partner of the Year Winner
PowerApps Award
2019 Partner of the Year Finalist
Modern Desktop Award
Power BI Award

2019 MSSP Partner Award Winner
Modern Workplace – Security and Compliance
Fail #1 Netflix Outage | Root Cause Analysis

- AWS inadvertently deleted US-East ELB configuration data
- Incoming traffic was not redirected to servers
- Streaming eventually was halted on most US devices
- AWS restored the ELB configuration that evening
- Outage affected millions of customers
- Netflix took the most damage to revenue and trust, not AWS
Anatomy Lessons Learned

>Detect
Which practices and procedures could have detected the incident early and mitigated damage?

>Prevent
What practices and methods will prevent similar incidents in the future?
Fail #1 Netflix Outage

- Remote monitoring indicated AWS outages
- Increase in user incident requests
- Sharp decrease in resource utilization
Fail #1 Netflix Outage > Prevent

- Define resiliency business objectives
- Define critical resources with SLO
- Create policy that critical resources are available in multiple regions (availability sets)
- Implement monitoring across all deployed regions
- Trailblaze DevOps innovations (Chaos Monkey)
Poll Question #1
Cloud is powerful, with challenges

- 44% of companies cannot keep track of cloud infrastructure
- 62% of cloud adopters reported faster access to application infrastructure
- 28% of IT professionals aren’t confident their cloud infrastructure is secure
- 50% of cloud services are deployed by Shadow IT
- 74% of IT expenses are dedicated to O&M

State of Cloud Infrastructure Governance 2017 Survey, commissioned by Fugue
https://www.itchronicles.com/governance/enterprise-cloud-infrastructure-governance/

Right Scale 2017
https://www.raconteur.net/technology/cloud-computings-next-phase-business-transformation
Fail #2  Cost Overrun

- Oil and gas company modernizing line of business apps to the cloud
- Using PaaS resources to allow for enhanced delivery and scaling
- 3 SQL Databases and a handful of web applications
- Internal TCO analysis estimated monthly spend at $10K, similar to on-premise spend
- Three months later, surprise invoice — double the consumption
Fail #2  Cost Overrun > Detect

- Manual inspection of spend
- Frequent cost reporting
- Wait for delayed invoice
- Spend alerts based on quotas
Fail #2 Cost Overrun > Prevent

- Define quotas for all applications
- IT brokers and assists product teams
- Implement automated provisioning that matches architecture
- Provide stakeholders frequent updates of current and projected spend
- Provide stakeholders current and projected cloud spend visibility
Fail #3  Cloud Storage Data Breach

• 2018 – FedEx subsidiary stored sensitive data on an open S3 bucket
• Exposed 7 years of customer data (2018 – 2015)
• 119,000 documents including passports, driver’s licenses, medical insurance, US military IDs
• Subject subsidiary was acquired in 2014
• FedEx inherited the risk exposure through M&A
Fail #3  Cloud Storage Breach > Detect

- Vulnerability scanning of all cloud resources
- Active and monitored IDS
- Monitoring unusual cloud resource activity
- Reviewing security settings on cloud resources
- Provide resource scanning for PII and privacy information
Fail #3  Cloud Storage Breach > Prevent

- Define cloud M&A onboarding strategy
- Define governance policies limiting public access to cloud resources
- Configure cloud policies to block (or audit) non-compliant configurations
- Implement an IDS
- Automate provisioning with polices enforced

Resource Management

Service Management

Security

Governance
Imagine

• You have an unlimited budget to build your own data center with NO UP FRONT COST
• You can add any service you want into your data center
• You have your top vendors building their services just for your data center
• The hardware and software is always up to date
• You only pay for what you use
Fail #4  Cloud Provider DC Outage

- FinTech ISV built consumer application on Azure PaaS resources
- Sept 2018 – Lighting brought down cooling in the Azure South Central data center
- Automated procedures to ensure hardware and data integrity began shutting down cloud resources
- Application is hosted in South Central data center, causing the application to become unavailable to all users
- ISV application outage lasted over 9 hours, resulting in > $100K lost revenue
Fail #4  Cloud Provider DC Outage > Detect

- Monitoring integration with cloud provider service data page
- Remote monitoring of web endpoints and real time alerting
- Detection of resource utilization reduction
Fail #4  Cloud Provider DC Outage > Prevent

- Define SLO objectives for availability
- Configure PaaS resources to leverage geo redundant capabilities
- Research app utilization to profile appropriate geo redundant data centers
- Configure remote and internal monitoring for all services
- Define and communicate incident response procedures upon cloud data center outage or degradation
Fail #5 Shadow IT

- Fortune 500 manufacturing/logistics company
- Goal: analyze and derive intelligence from ERP data
- Internal development team specified cloud-based Hadoop and search platform
- Internal IT, new to cloud, needed additional information and time to research solutions
- Development team, up against a deadline, created and deployed software to their own cloud accounts
- Unsanitized and confidential data leaked to public through public report endpoint
Shadow IT is very difficult to detect through cloud operations.

Internal controls such as network monitoring and locking down data can help, however, difficult to implement.

Cloud Shadow IT Users are not the enemy.
Fail #5 Shadow IT > Prevent

- Establish technology choices early during product business case development
- Define policies for approved cloud resources and configure
- Assist cloud users with evaluating cloud frameworks and configuring environment
- Provide turnkey reference architectures for cloud deployment
- Deploy service catalog with automation for rapid cloud provisioning
Fail #6  When Governance is not Governance

• Oil and Gas Company
  • Agility is key to their business plan

• Worked with Catapult to put in a governance plan for Azure

• Never looked at governance plan again

• First year spend $50,000

• 3rd year spend exceeded $1.5 million

• Rapid growth lead major cloud operations challenges

• Operational burden outweighed agility
Fail #6 Governance > Detect & Prevent

- Have a governance plan that everyone agrees with
- Set up monthly review of the governance plan
- Set up a cloud maturity model
- Align roadmap with governance plan
- Implement resource management per the governance plan
- Align strategy with financial management plan
- Set up a financial management plan and review quarterly
Poll Question #2
Governance: Compliance | Policy | Roles | Risk Management

<table>
<thead>
<tr>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Ad Hoc</td>
<td>Opportunistic</td>
<td>Systematic</td>
<td>Measured</td>
<td>Optimized</td>
</tr>
</tbody>
</table>

- No governance or policies in place
- Applicable regulations and compliance framework identified
- Organizing subscriptions using Azure Management Groups
- Rough outline of scaffold
- Define and prioritize security controls
- Developing policies for critical priority controls
- Cloud roles align with enterprise identity management roles
- Buy in of governance policies across organization
- Azure scaffold complete
- Policy coverage for moderate and critical controls
- Active auditing of compliance
- Frequent notification of policy violations
- New accounts and subscriptions automatically inherit policy
- Auditing and alerting on policy violations
- Policy violations are decreasing over time
- Policies in blocking policy violations
- Policy metrics included in executive and business KPIs

PRACTICE LAUNCH

SETTING TARGETS

REALIZING BENEFITS

QUANTIFIABLE

GOLD STANDARD

Capability, operational excellence, and quality increase as higher maturity levels are realized.
Key Takeaways

• Cloud success defines strategic vision and goals
• Governance provides a framework and guardrails
• Build in security from the beginning, based on governance
• Service management is important to operate a healthy cloud
• Resource management (the fun part) needs to come after DD into Strategy, Governance, and Security
• Establish an internal, performant, and reliable, brokerage practice to enable enterprise cloud users and curtail Shadow IT
• Cloud is a powerful platform that provides amazing opportunities
3 Days | 2 Cloud Experts | 1 Topic of Your Choosing

Spend 3 days with 2 Catapult cloud experts, helping you improve 1 area of your Azure environment. Choose one of the following topics:

- Financial Management
- Governance & Security

Contact Larry Swonke for more information: Larry.Swonke@catapultsystems.com