

## Cloud Insecurity: The Need for Stronger Identity Management



Should you entrust your private keys in the cloud? Eighty percent of companies store information in the public cloud, begging the question of cloud security. The cloud promises availability, simplified management, and cost savings — yet, the cloud is not threat-proof and opens new attack vectors. Organizations need to proceed with caution about what they store.

To ask a question, use the green “Q&A” button on the left side of your screen. All questions are anonymous.



Mark B. Cooper  
president and founder, PKI Solutions



[mark@pkisolutions.com](mailto:mark@pkisolutions.com) | [@thepkiguy](https://twitter.com/thepkiguy)

Mark B. Cooper, president and founder of PKI Solutions, is known as “The PKI Guy” since his early days at Microsoft. He has deep knowledge and experience in all things Public Key Infrastructure (PKI). PKI Solutions Inc. provides consulting, training — including online training — and implements software solutions for Microsoft PKI and related technologies at enterprises, many of them Fortune 500 companies. PKI Solutions has led hundreds of PKI trainings, including private trainings, across the country and around the world.



- President and Founder, PKI Solutions
- Known as “The PKI Guy” since early days at Microsoft
- Leading PKI subject matter expert
- At PKI Solutions, we implement PKI solutions at enterprises
- I lead hundreds of PKI trainings from Scotland to Buffalo, Sweden to Portland
- In-person and online trainings available
- My focus is security, PKI design and implementation, identity management

## What Are We Talking About Today?

- Hidden dangers of cloud security
- Learn how to minimize risks in the cloud
- What to ask your cloud provider
- Learn best practices for storing private keys, keeping them secure
- Learn how to build and align your security practices and controls around virtualized environments





## Agenda

- Current cloud security landscape
- Understanding cloud security issues
- Data and identity management: what's at stake
- Threats, flaws, vulnerabilities, risks
- What not to store in the cloud
- Ownership, control, responsibilities
- On-premise vs. cloud storage vs. hybrid options
- The pitfalls of poor cloud management
- Best practice checklist
- Q&A



## Current Cloud Security Landscape



**77%** of all enterprises have a portion of their infrastructure in the cloud

**83%** of enterprises workloads will be in the cloud by 2020

### But...

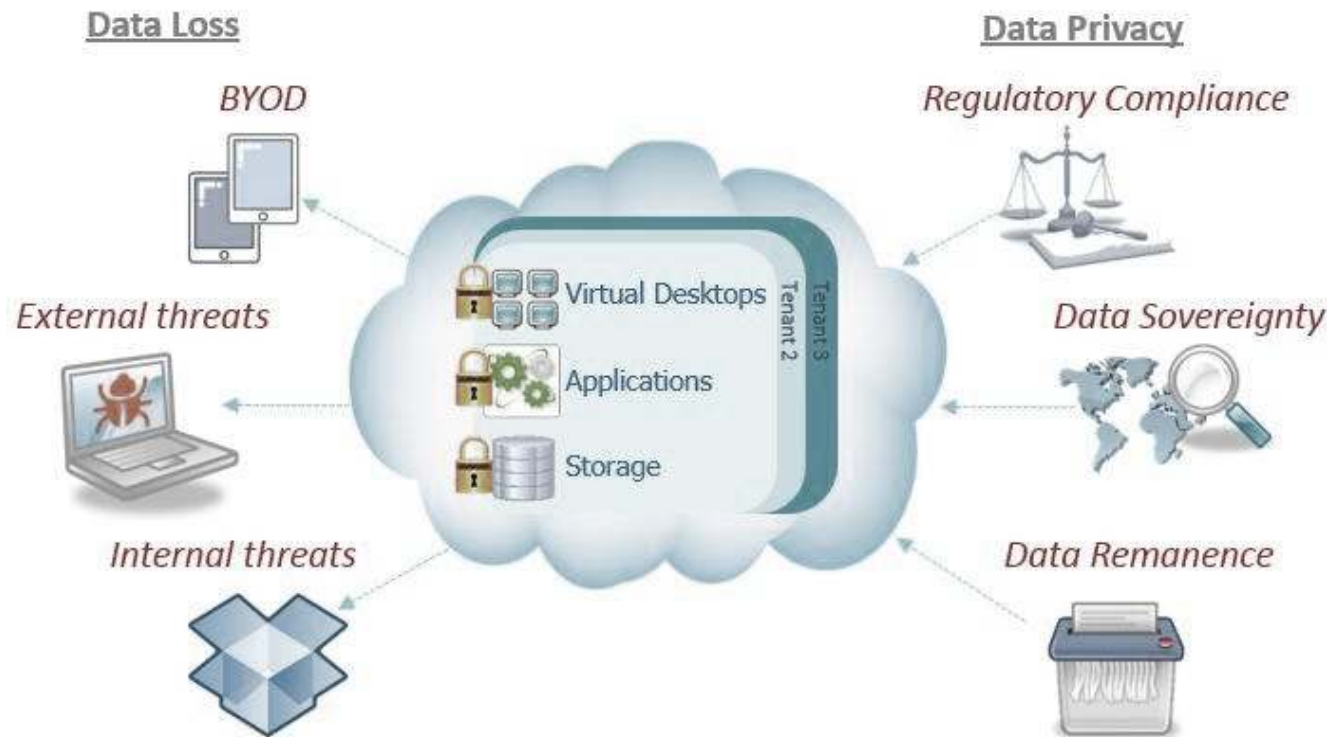
- Case law and integrity claims have yet to be vetted
  - International Exposure
  - Data disclosure through direct and indirect investigations
- Lack of consistent standards and still evolving
  - Multi-Factor Authentication (MFA)
  - Certificates via PKI

## The Pitfalls of Poor Cloud Management

- Account compromise
- Network compromise
- Information leak
- Data breach
- Outages
- Compliance issues
- Loss of reputation
- Business shutting down
- Encryption key compromise
- Inadvertent disclosures



## Understanding Cloud Security Issues





## Data and Identity Management: What's at Stake

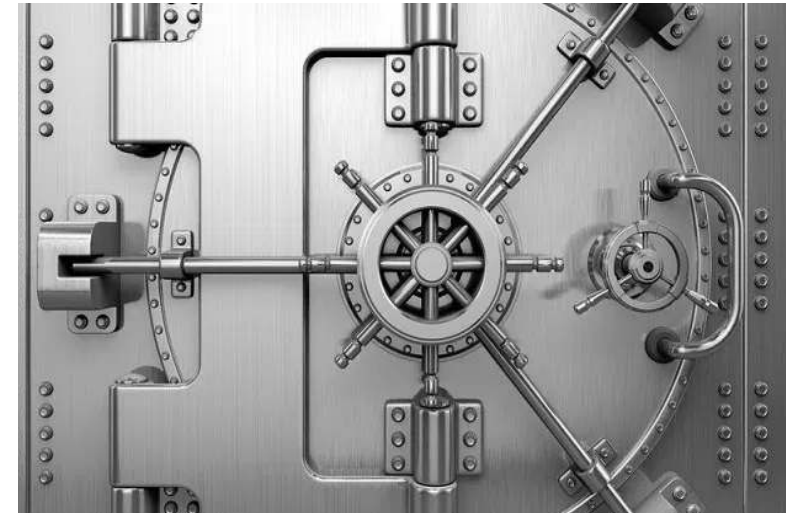
**PKI**  
SOLUTIONS

Cloud **cryptojacking** malware is one of the biggest threats in 2019.

- **Bottom line:** Stronger identities lead to stronger data protections!

## Threats, Flaws, Vulnerabilities, Risks

- Physical Tokenization and crypto vaults are the only way to increase security
- Vulnerabilities
  - Data breach
  - Data loss
  - Hijacking
  - Insecure interfaces and APIs
  - DoS
  - Insufficient due diligence
  - Shared technology vulnerabilities





## What Not to Store in the Cloud

- Passwords
- Unencrypted data
- Encryption Keys
  - Symmetric
  - Asymmetric (Private)
- Cryptocurrency wallets
- SQL connection strings
- Storage account keys
- API tokens

**PKI**  
SOLUTIONS



**PKI**  
SOLUTIONS

Own all data and identities

Control access

Assign ownership



## On-Premise vs. Cloud vs. Hybrid Options

- Data and services in the cloud
- Managed service
  - Vaulting and key storage landscape is changing
- Cloud service key management
  - Cloud provider
  - Neutral third party
  - Hybrid with on-premises

**PKI**  
SOLUTIONS

## Best Practice Checklist

- ✓ Place secrets in private repository
  - ✓ Independent of data storage provider
- ✓ Central
  - ✓ Vaulting, key management, auditing
- ✓ Restricted access
- ✓ Separate data from secrets/keys
  - ✓ Use location to your advantage. Secrets on premises, data in the cloud
- ✓ Keep data encrypted using keys
- ✓ Ensure keys are encrypted at rest





# QUESTIONS?



## THANK YOU FOR JOINING US!

Mark B. Cooper, president and founder, PKI Solutions

[mark@pkisolutions.com](mailto:mark@pkisolutions.com)  
[@ThePKIGuy](https://twitter.com/ThePKIGuy)