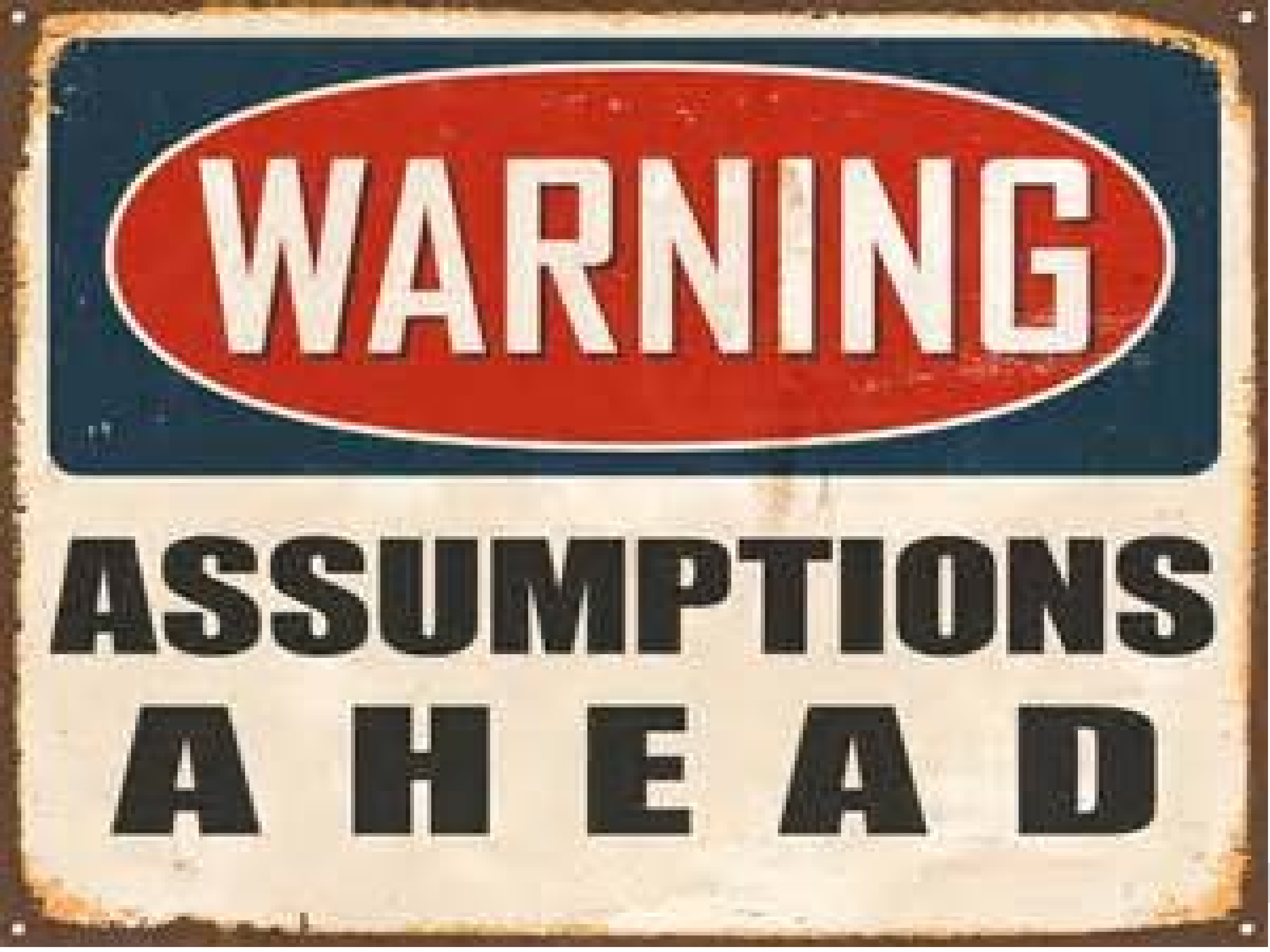
PLOTTING YOUR DATA EXIT BEFORE ENTERING THE CLOUD

FREDRIK FORSLUND

DIRECTOR, CLOUD & DATA CENTER ERASURE SOLUTIONS, BLANCCO TECHNOLOGY GROUP

atlantic
BritWeek
virgin
AEG
TRAD
INVESTM
virgin atl



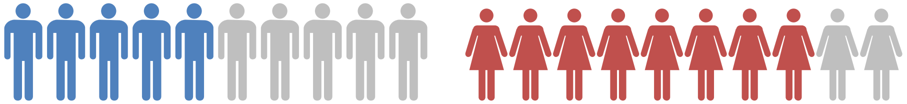
WARNING

ASSUMPTIONS

AHEAD

Assumption #1: Cloud Storage Providers Should Take Care of *Your* Needs

- ✓ Loss of control and ownership
- ✓ Lack of visibility into what’s stored in the cloud
- ✓ Unauthorized mobile/connected devices accessing the cloud
- ✓ Lack of visibility into security practices
- ✓ Failure to personally conduct regular audits or have regulatory agencies conduct them



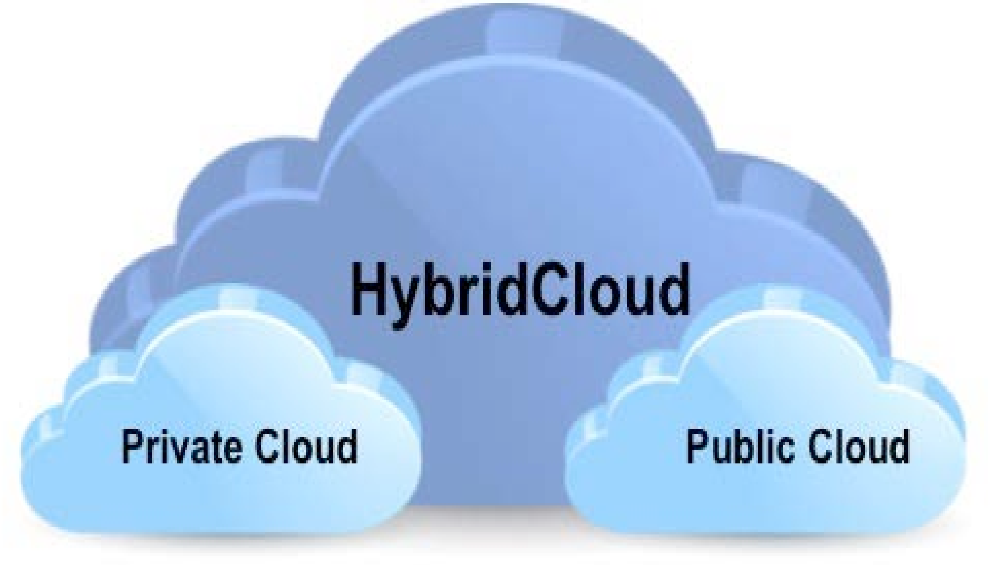
Assumption #2: It’s Easy to Hack into the Cloud

- ✓ Seen as ‘fruit bearing jackpot’ by hackers
- ✓ Sophisticated hacker groups leveraging global technology and expertise are the ‘new normal’
- ✓ Flatness and openness of cloud make it more vulnerable
- ✓ Unaware of how and where attackers can infiltrate systems

Assumption #3: Insider Threats Are Few and Far Between

- ✓ Employees leave organization – and take access to cloud servers with them
- ✓ Accidental mistakes made by current employees due to lack of training
- ✓ Internal administrators accessing executive-only intellectual property/financial statements
- ✓ Current employees access cloud data with the intention of leaking for monetary gain

Assumption #4: A Hybrid Cloud Strategy Is the Sweet Spot



- ✓ Scalability
- ✓ Lower infrastructure costs
- ✓ Freedom to innovate
- ✓ But...are security risks and inefficiencies minimized?

Assumption #5: Politics & Government Don't Impact Your Cloud Strategy

- ✓ Aug 2015: FTC has authority to regulate corporate cyber security
- ✓ Dec 2015: Obama signs $1.1 trillion cyber security spending bill
- ✓ Dec 2015: EU GDPR requirements are finalized
- ✓ April 2016: EU-US Privacy Shield creates new legal framework for transatlantic data flows to protect fundamental rights of Europeans where their data is transferred to U.S. and ensure legal certainty for businesses

Assumption #6: You Only Have To Anticipate the Contentious Breakups

- ✓ Prices go up and you can no longer afford it
- ✓ Contract renewal terms aren’t desirable
- ✓ Services aren’t up to par
- ✓ Security isn’t as strong as you thought
- ✓ A different vendor can do the job better

https://www.youtube.com/watch?v=BrV-SXI6Nmo

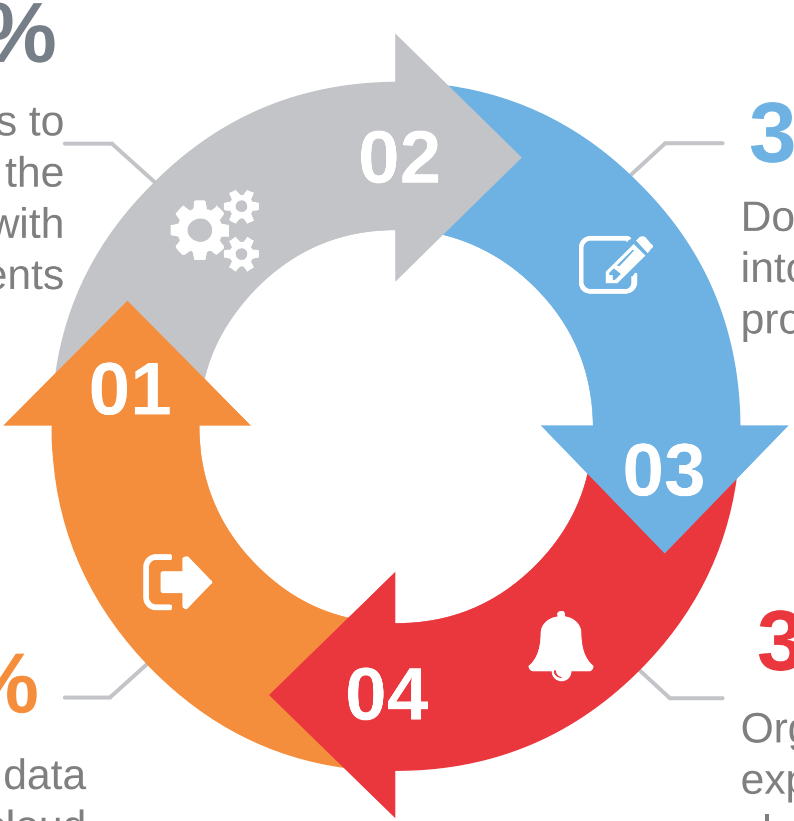
The Cloud Storage Struggle Is Very Real

40%

Cite unauthorized access to data from other tenants as the most pressing concern with public cloud deployments

33%

Do not currently have visibility into their public cloud providers' operations



40%

Store or process sensitive data in the cloud

33%

Organizations that experienced breaches in the cloud cited malware as the top private cloud attack vector

**Source: SANS Institute, 'Orchestrating Security in the Cloud' Paper, 2015*

6 Scenarios When Data Removal Is *Absolutely* Necessary

Sending Back Drives for Warranty

Terminating Virtual Machines in IaaS Cloud

Planned SAN/Server Decommissioning

Disaster Recovery Exercises

Planned Data Migration & Data Center Consolidation

Regulation/Governing Bodies Conduct Audits

Scenario #1: Sending Back Faulty Drives Under Manufacturer Warranty

Security policy stops drives from leaving data center

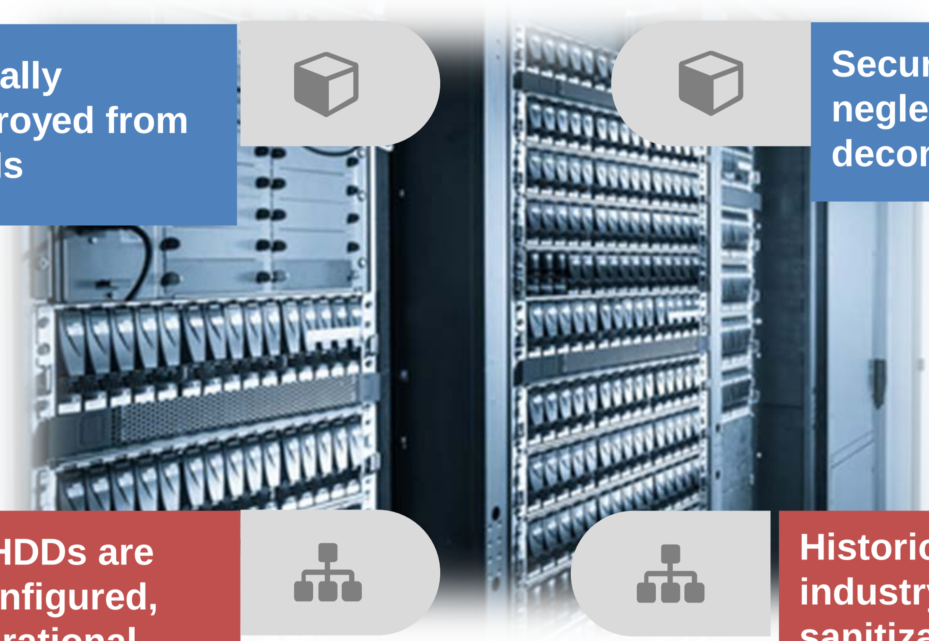
Expensive contracts with drive manufacturers to “keep my drive” + physical destruction costs

Sending Back Faulty Drives Under Manufacturer Warranty: Doing It the *Right* Way

What You Should *Really* Do: Securely erase drives first, then send back drives under warranty

What's the Benefit to *You*: Cost savings, minimized data exposure and compliance readiness

Scenario #2: Planned SAN/Server Decommissioning



HDDs are physically removed or destroyed from storage and SANs

Security policy often neglects guidance on decommissioned SANs

Individual SAN HDDs are erased and reconfigured, adding onto operational costs

Historically there was no industry standard for “data sanitization” of storage area networks

Planned SAN/Server Decommissioning: Doing It the *Right* Way

What You Should *Really* Do: Remotely erase SANs while in active use, erase all active LUNs containing customer data

What's the Benefit to *You*: Minimized security risks, regulatory compliance readiness (with audit trail), increased revenue through resale of equipment

Scenario #3: Planned Data Migration & Data Center Consolidation

Data in internal infrastructure is often left behind after data migration

Remote employees still need to access CRM and ERP applications, which access personally identifiable data

There is no process for the transition period – when new customers replace previous ones on existing infrastructure

Resolving outages and other issues often requires a physical presence

Planned Data Migration & Data Center Consolidation: Doing It the *Right* Way

What You Should *Really* Do: Securely erase dedicated storage on the logical level before reassigning the storage

What's the Benefit to *You*: Holistic data management across entire lifecycle, minimized security risks and regulatory compliance readiness (with audit trail)

Scenario #4: Terminating Virtual Machines in the IaaS

Remote employees still need to access CRM and ERP applications, which access personally identifiable data

Resolving outages and other issues often requires a physical presence

Terminating Virtual Machines in the IaaS: Doing It the *Right* Way

What You Should *Really* Do: Integrate with the Hypervisor and get information on all files related to the VM and then securely erase them.

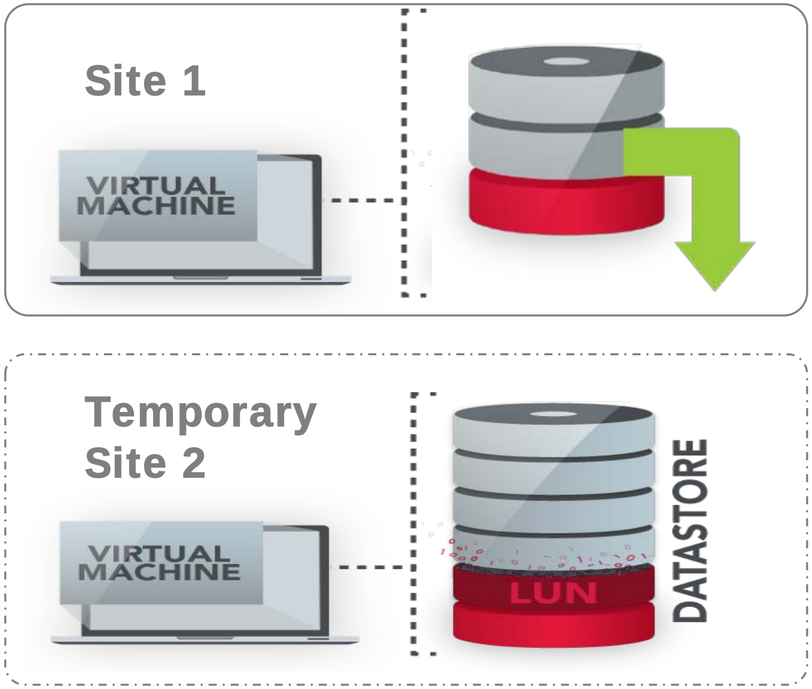
What's the Benefit to *You*: Protection against data breaches, active information life cycle management with full audit trail.

Scenario #5: Disaster Recovery Data Exercises

Disaster recovery data exercises are regularly performed for customers

There is rarely any established processes or documentation for securely erasing live data

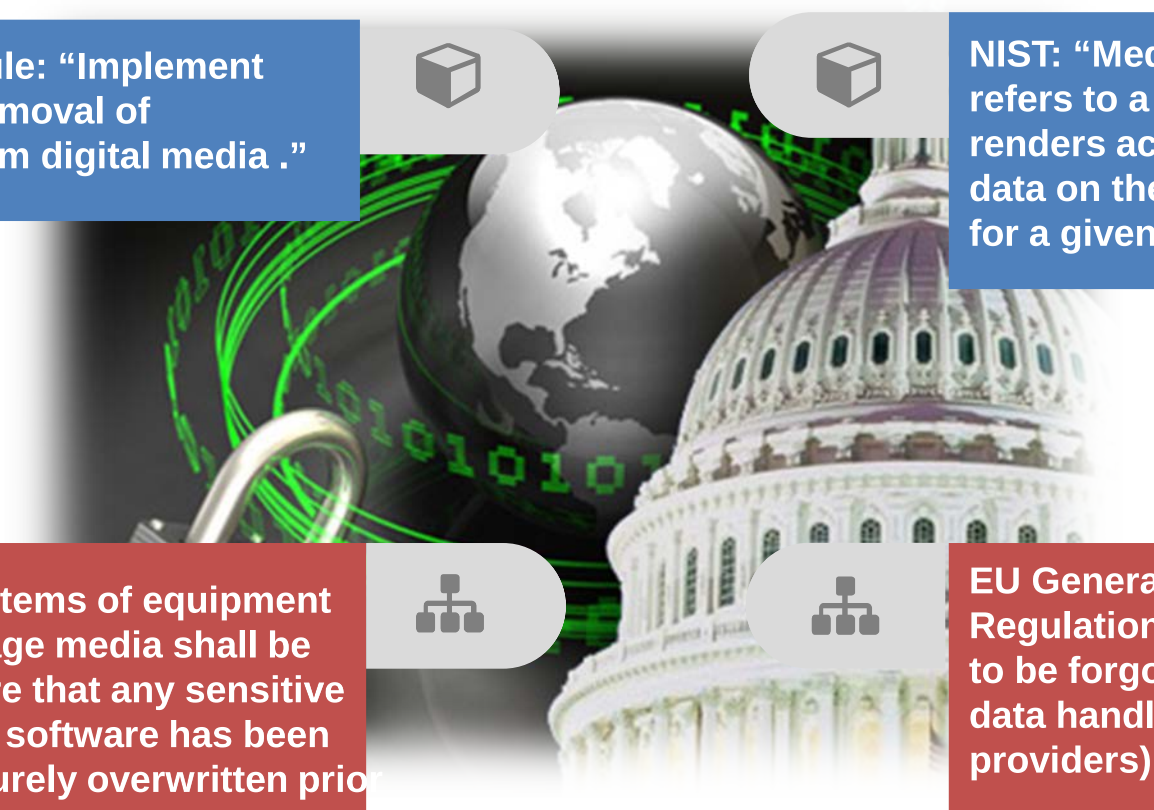
Disaster Recovery Data Exercises: Doing It the *Right* Way



What You Should *Really* Do: Erase customer data from temporary sites (post disaster recovery exercise), integrate proof of erasure into process

What's the Benefit to *You*: Minimized data exposure/loss, evidence for regulatory compliance, revenue generation

Scenario #6: Regulatory/Governing Bodies Conduct Audit



HIPAA Privacy Rule: “Implement procedures for removal of electronic PHI from digital media .”

NIST: “Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort.”

ISO 27001: “All items of equipment containing storage media shall be verified to ensure that any sensitive data or licensed software has been removed or securely overwritten prior to disposal or reuse.”

EU General Data Protection Regulation requires the “right to be forgotten” and applies to data handlers (i.e. cloud providers)

Cloud Magna: A Cloud Storage Success Story

http://www.blancco.com/en/content/cloud-magna-customer-success-story

Content You May Find Useful:

“Cloud & Data Center Erasure: Why Delete Doesn’t Suffice”: http://www2.blancco.com/en/white-paper/cloud-and-data-center-erasure-why-delete-doesnt-suffice

“The Information End Game: What You Need to Know to Protect Corporate Data Throughout its Lifecycle”: http://www2.blancco.com/en/white-paper/the-information-end-game-what-you-need-to-know-to-protect-corporate-data

“Data Storage Dilemmas & Solutions”: http://www.slideshare.net/BlanccoTechnologyGroup/data-storage-dilemmas-solutions

“EU GDPR: A Corporate Dilemma”: http://www2.blancco.com/EU-GDPR-Corporate-Dilemma-Research-Study