Data End of Life in the Cloud: Why, When and How?

Fredrik Forslund,
Director - Cloud and Data Center Erasure Solutions,
Blancco Group
Two young guys...
...erasures every day.
“Media **sanitization** refers to a process that renders access to target data on the media infeasible for a given level of effort.”
What is Certified Data Erasure?

Format or Delete

Data Erasure
Data End of Life—broader definition

- Erasure technology choice
- Process implementation and verification
- Reporting and audit trail
Why?
Many current drivers!

- National Data Protection Law
- EU Data Protection Regulation 2015/16
- "Right to Erasure"
- ISO Standard 27001
- PCI-DSS
- HIPAA Compliance
- Credit Card Industry PCI-DSS
- (Health Insurance Portability and Accountability)
- Sarbanes-Oxley
Government initiatives
Cloud Industry recommendations

“Include data end-of-life (erasure) with auditable reporting into your cloud security eco system”

Data Life Cycle
According to the Cloud Security Alliance, it falls to “…the provider to keep that data secure, and when it is deleted, the provider should ensure (or be able to prove) that it is permanently destroyed.”
A San Francisco Case

Corporate facts:


• One of the largest AWS S3 customers.

• Running tens of thousands of servers in multiple data centers.

• Managing hundreds of billions of files and growing.

• Founded by Drew Houston and Arash Ferdowsi.
“Dropbox uses secure deletion process to delete data once a customer has permanently deleted a file from their Dropbox account or after service termination. When a Dropbox storage disk has reached the end of its useful life or is damaged, we follow a decommissioning process that is designed to destroy the disk to the point data cannot be reasonably recovered. Our managed service provider also follows secure destruction processes for media they control.”
Section A.11.2.7 "Secure disposal or re-use of equipment" - "All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."

Section A.18.1.4 “Privacy and protection of personally identifiable information”

Section A.14.3.1 "Protection of test data"
Telehouse case

46 sites in 24 cities, 13 countries
As Datacenter and Cloud solution provider, Telehouse is committed to providing strong guaranty to its customer. We chose a software based data erasure process as a irrefutable evidence that we comply with EU regulation when deleting Customer data.

More than a technical solution the software erasure process allows us to deliver **TRUST** to our Customer. This is the most valuable asset in our business field, on top of providing strong evidence for our security certifications like ISO 27001 or PCI DSS". 

Benoît Mercier
Directeur ICT Solutions
Telehouse Europe
threats- internal

case study – deleted virtual disks

• initial facts
  • 28 lun's (28 datastores)
  • 440 vmdks
  • 1000+ snapshots

• additional information
  • exchange, sql, oracle, file servers all gone
  • backups also deleted
Ex-NSA director: China has hacked 'every major corporation' in U.S.

Mike McConnell, when he was still national director of intelligence at the tailend of the Bush administration.

The Chinese government -- seeking to steal valuable secrets -- has hacked into the computers at every major American company,
When?
PROCESS EXAMPLE:

#1 SAN decommissioning

- HDD level or LUN level
- Functioning or not after Erasure
- Locally or remotely
- Auditable
PROCESS EXAMPLE:

#2 Extra Data

- Disaster recovery exercises
- Test data
- Actual disasters
- Auditable
PROCESS EXAMPLE:

#3 Data Entry

- Data in original sites
- Temporary sites
- Auditable
#4 Data Migration and Data Exit

- Data migration policy
- Secure Data Exit
- Auditable
All the “whens” will need to be defined in your service contracts.

Dropbox, now for your business.

“Dropbox customers retain control and ownership of their data and are responsible for enforcing their data retention policies according to their requirements. Dropbox for Business provides administrators and users with the ability to permanently delete their data.”
How?
Erasure levels:

**Erasure on File, Logical and Virtual Levels:**

- VIRTUAL Erasure
- LUN Erasure
- FILE Erasure

**Total Erasure on physical level:**

- SERVER Erasure
- DISK Erasure (HDD and SSD)
Physical Level

Virtual Machines/Servers and vApps (grouped VMs) hosted on various hypervisors

Logical Storage (LUNs)

Logical Unit Numbers (LUNs) viewed as virtual drives dedicated to data storage on Storage Area Networks (SANs)

Data Erasure as a Service (DEaaS)
Final Comments!
What not to do!

A Norwegian Data End of Life Process...
Reuse! instead of retire and destroy.

- Significant value for someone within your own organization
- Might help an external organization in your community
- Might help an organization abroad in a developing region

88%
Connect! Or e-mail: fredrik.forslund@blancco.com
Thank you...