
Session Title:
Data Destruction Best Practices to Mitigate Data Breach Risks
Speaker Name:
Sunil Chandna, CEO Stellar
stellar
iaitam.org | Peace, Love & Asset Management | ACE 2022

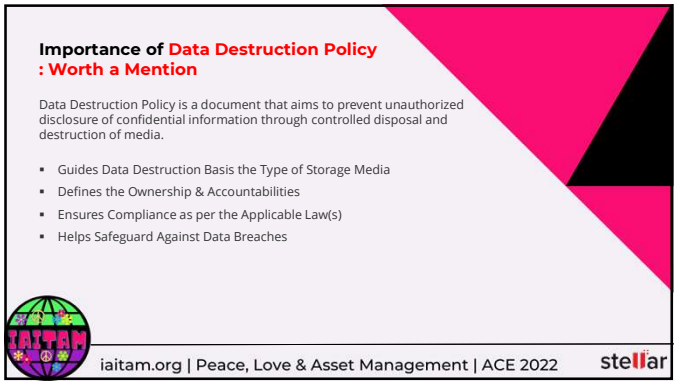
1


LET'S TALK!
Data Destruction Best Practices to Mitigate Data Breach Risks
SESSION INSIGHT
Understand Data Destruction Challenges Faced By Organizations
Importance of Data Destruction Policy
Best Practices For Data Destruction and Its Benefits
Key Considerations For IT Asset Managers
stellar
iaitam.org | Peace, Love & Asset Management | ACE 2022

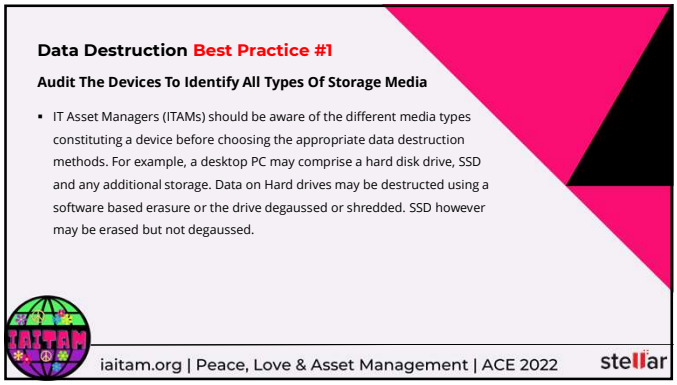
2


Data Destruction Challenges Faced By Organizations Today!
Ever Growing Data Stored On Multiple Devices
Lack Of Structured Data Destruction Policy In Place
Improper Data Lifecycle Management
Missing Or Inadequate Controls
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

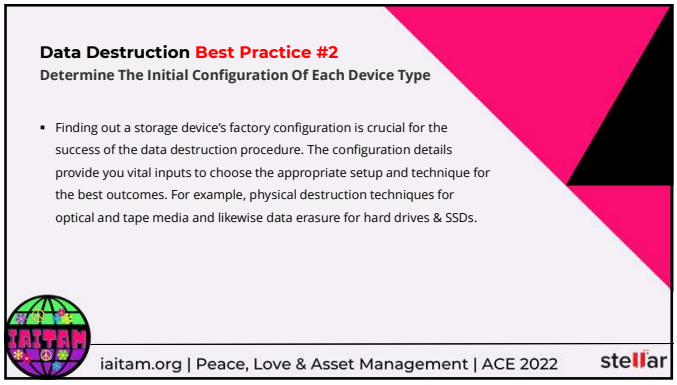
3


Importance of Data Destruction Policy
: Worth a Mention
Data Destruction Policy is a document that aims to prevent unauthorized disclosure of confidential information through controlled disposal and destruction of media.
Guides Data Destruction Basis the Type of Storage Media
Defines the Ownership & Accountabilities
Ensures Compliance as per the Applicable Law(s)
Helps Safeguard Against Data Breaches
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

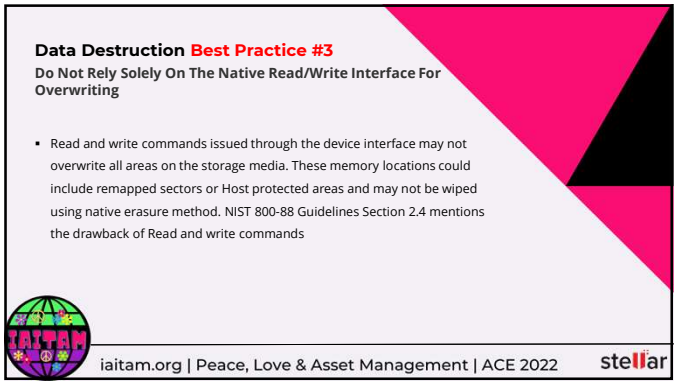
4


Data Destruction Best Practice #1
Audit The Devices To Identify All Types Of Storage Media
IT Asset Managers (ITAMs) should be aware of the different media types constituting a device before choosing the appropriate data destruction methods. For example, a desktop PC may comprise a hard disk drive, SSD and any additional storage. Data on Hard drives may be destructed using a software based erasure or the drive degaussed or shredded. SSD however may be erased but not degaussed.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

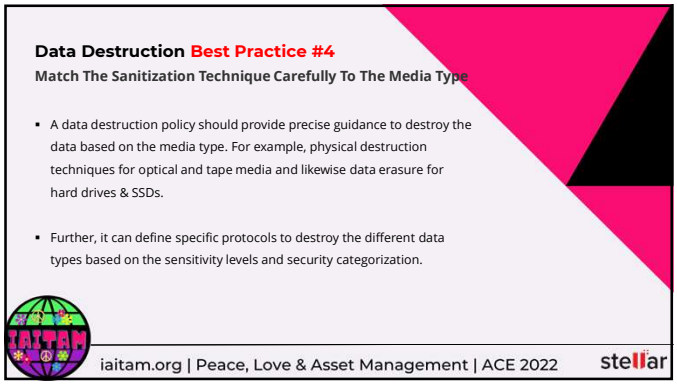
5


Data Destruction Best Practice #2
Determine The Initial Configuration Of Each Device Type
Finding out a storage device's factory configuration is crucial for the success of the data destruction procedure. The configuration details provide you vital inputs to choose the appropriate setup and technique for the best outcomes. For example, physical destruction techniques for optical and tape media and likewise data erasure for hard drives & SSDs.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

6


Data Destruction Best Practice #3
Do Not Rely Solely On The Native Read/Write Interface For Overwriting
▪ Read and write commands issued through the device interface may not overwrite all areas on the storage media. These memory locations could include remapped sectors or Host protected areas and may not be wiped using native erasure method. NIST 800-88 Guidelines Section 2.4 mentions the drawback of Read and write commands
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

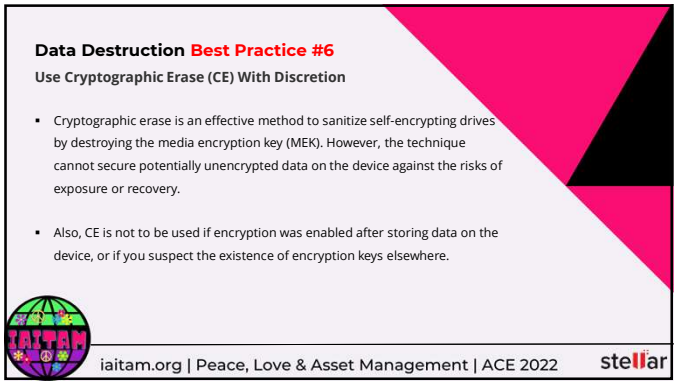
7


Data Destruction Best Practice #4
Match The Sanitization Technique Carefully To The Media Type
▪ A data destruction policy should provide precise guidance to destroy the data based on the media type. For example, physical destruction techniques for optical and tape media and likewise data erasure for hard drives & SSDs.
▪ Further, it can define specific protocols to destroy the different data types based on the sensitivity levels and security categorization.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

8


Data Destruction Best Practice #5
Avoid Using Degaussing To Sanitize The Evolving Magnetic Media
▪ The degaussing technique faces inherent challenges to sanitize the emergent magnetic storage media. Firstly, the evolving magnetic storage devices have stronger coercivity, hindering the existing degaussers from sufficiently demagnetizing them to attain data destruction.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

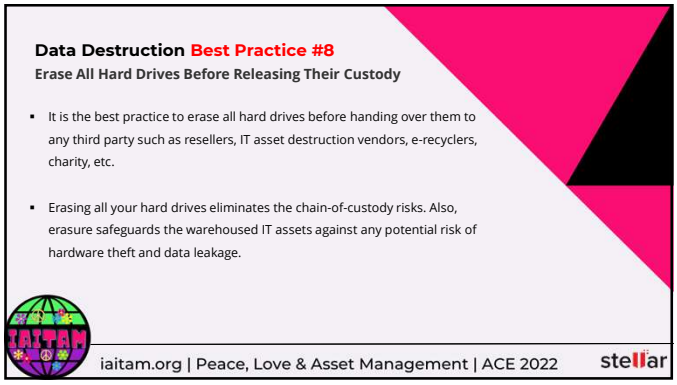
9


Data Destruction Best Practice #6
Use Cryptographic Erase (CE) With Discretion
Cryptographic erase is an effective method to sanitize self-encrypting drives by destroying the media encryption key (MEK). However, the technique cannot secure potentially unencrypted data on the device against the risks of exposure or recovery.
Also, CE is not to be used if encryption was enabled after storing data on the device, or if you suspect the existence of encryption keys elsewhere.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

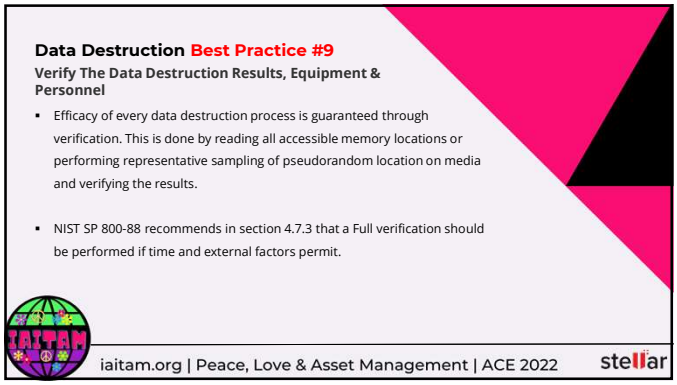
10


Data Destruction Best Practice #7
Perform Full Media Sanitization Instead of Partial Sanitization
In partial media sanitization scenarios there is no definite way to ensure that all the sensitive target data is effectively destroyed.
Sometimes, an organization may prefer sanitizing a subset of the storage media instead of destroying the complete data. For e.g., a hard drive on a server may store the data of several customers at a time and the company may prefer destroying the data of only the churned customers while retaining the rest of the data on other storage areas on the drive. So Full media sanitization is recommended.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

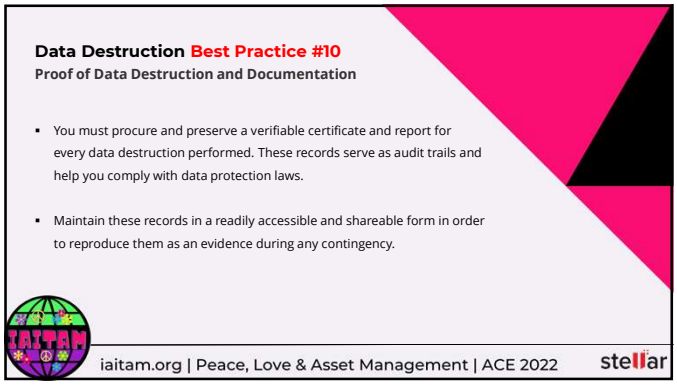
11


Data Destruction Best Practice #8
Erase All Hard Drives Before Releasing Their Custody
It is the best practice to erase all hard drives before handing over them to any third party such as resellers, IT asset destruction vendors, e-recyclers, charity, etc.
Erasing all your hard drives eliminates the chain-of-custody risks. Also, erasure safeguards the warehoused IT assets against any potential risk of hardware theft and data leakage.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

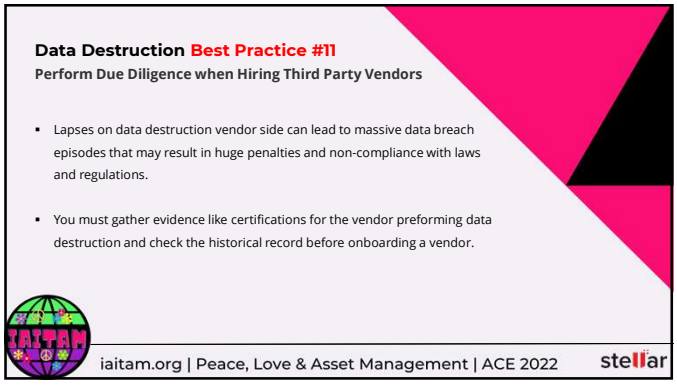
12


Data Destruction Best Practice #9
Verify The Data Destruction Results, Equipment & Personnel
Efficacy of every data destruction process is guaranteed through verification. This is done by reading all accessible memory locations or performing representative sampling of pseudorandom location on media and verifying the results.
NIST SP 800-88 recommends in section 4.7.3 that a Full verification should be performed if time and external factors permit.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

13


Data Destruction Best Practice #10
Proof of Data Destruction and Documentation
You must procure and preserve a verifiable certificate and report for every data destruction performed. These records serve as audit trails and help you comply with data protection laws.
Maintain these records in a readily accessible and shareable form in order to reproduce them as an evidence during any contingency.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

14


Data Destruction Best Practice #11
Perform Due Diligence when Hiring Third Party Vendors
Lapses on data destruction vendor side can lead to massive data breach episodes that may result in huge penalties and non-compliance with laws and regulations.
You must gather evidence like certifications for the vendor preforming data destruction and check the historical record before onboarding a vendor.
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

15


Benefits of Data Destruction Best Practices
Ensures Permanent Destruction
Helps Maintain Compliance
Ensures Data Security & Brand Protection
Reduce Data Breach Risks
Prevent Hefty Fines and Penalties
Helps Protect Environment & Achieve Sustainability
Peace of Mind
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

16


Key Considerations For IT Asset Managers
IT Asset managers must consider the following while adopting best data destruction practices.
Functional Efficacy
Costs Consideration
EHS (Environment, Health & Safety) Impact
Regulatory Compliance
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

17


Best Practices of Data Destruction Summarized
Audit The Devices To Identify All Types Of Storage Media
Determine The Initial Configuration Of Each Device Type
Do Not Rely Solely On The Native Read/Write Interface For Overwriting
Match The Sanitization Technique Carefully To The Media Type
Avoid Using Degaussing To Sanitize The Evolving Magnetic Media
Use Cryptographic Erase (CE) With Discretion
Perform Full Media Sanitization Instead of Partial Sanitization
Erase All Hard Drives Before Releasing Their Custody
Verify The Data Destruction Results, Equipment & Personnel
Proof of Data Destruction and Documentation
Perform Due Diligence when Hiring Third Party Vendors
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

18


Thank You
✓ You may Download a copy from our website:
https://www.bitraser.com/knowledge-series/
iaitam.org | Peace, Love & Asset Management | ACE 2022
stellar

19