BRAINSTORM
2019

Critical Data Destruction:
What IT Leaders Need to Know

Topics

- Where data is stored
- When data needs to be destroyed
- Why data needs to be destroyed
- NIST 800-88: Guidelines for Media Sanitization – a framework for a comprehensive data destruction program
- Environmental challenges
- Reuse value

Where data is stored

When data needs to be destroyed

Internal redeployment

- » Employee changes
- » Business changes

Repair/Replace – internal or external

- » Scheduled refresh
- » Break/fix

Disposal – leave organization

- » ITAD vendor
- » Lease returns
- » Donations, employee sales

CASCADE ASSET MANAGEMENT

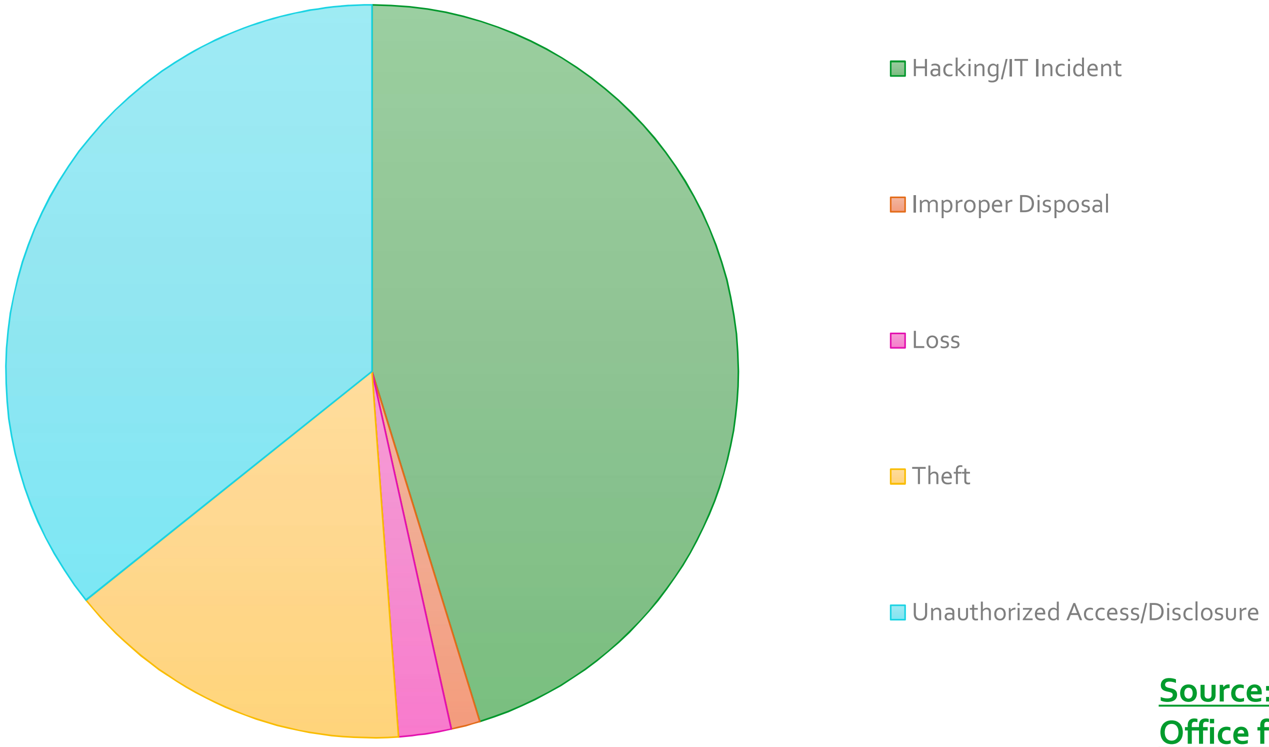
BrainStorm FOR ED TECHS, BY ED TECHS EDUCATIONAL TECHNOLOGY CONFERENCE 2019

Why data needs to be destroyed

- Prevent data breach
- Comply with law: HIPAA, FACTA, etc.
- Organizational Policy
  - Risk Assessment – where are you at risk from a data breach?
    - §164.308(a)(1)(ii)(A) Risk analysis (Required): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate

(Security Rule of HIPAA, 1996)

Why data needs to be destroyed



19% of reported breaches

Source: U.S. Dpt. of Health and Human Services Office for Civil Rights

Consistent elements of compliance:

- The reasonableness standard
- Designation of accountability
- Written procedures and employee training
- Vendor selection due diligence

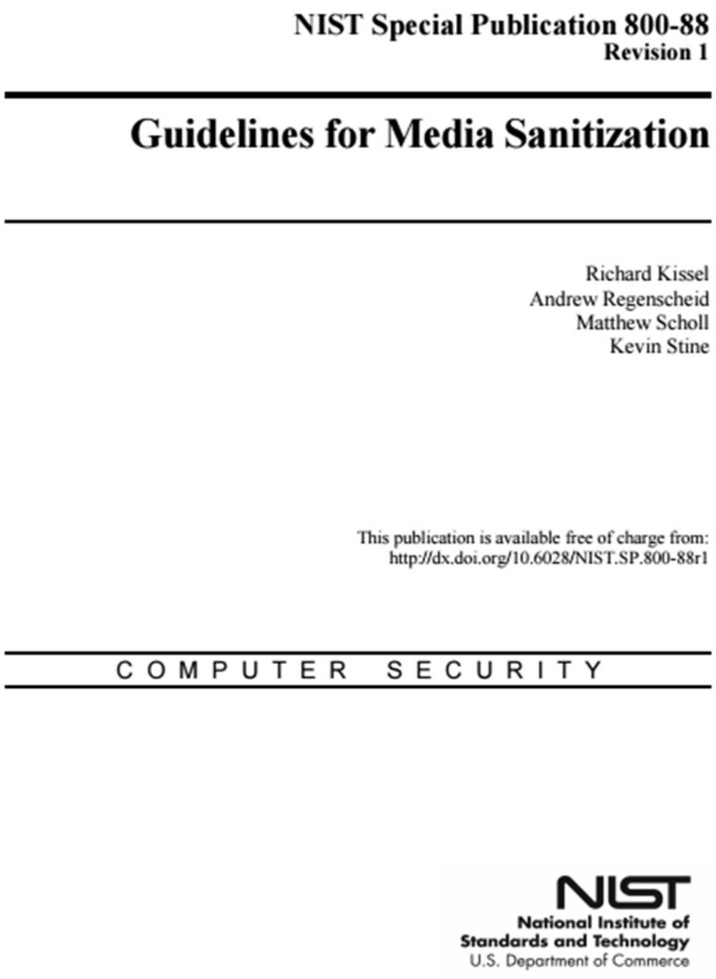
Data Protection Policy

Set policy for managing data on retired/reused assets

- » Comprehensive review of what data bearing devices you own and manage
- » Develop and implement training and controls (including destruction) consistent with policy
- » Ensure proper implementation within and outside of the organization's control

NIST 800-88

"This guide will assist organizations…
in making practical sanitization decisions
based on categorization of information"



NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST 800-88

- Practical, real world reference for media sanitization guidance and compliance
- Introduced in 2006, updated Dec, 2014 (Revision 1) to address changing technologies
- Replaced DoD 5220.22M standard in regulatory and certification practice
- Referenced in many other security rules, regulations and standards

How to destroy data

Electronic sanitization

- Over-writing
- Cryptographic erase

Physical destruction

- Degaussing magnetic media
- Shredding (shred size depends on media)
- Bending, waffling
- Melting

Media sanitization

is a process by which data is irreversibly removed from media or the media is permanently destroyed.

Note:

NIST considers any of these forms of data destruction as a type of "Sanitization."

Destroy On-Site or Off-Site?

Crucial factors:

» Physical security - Staging of materials prior to disposition

» Transfer/transport of media

» Electronic media collection and staging

- Tagging and tracking assets
- Off-site destruction – vendor selection
- Reconciliation of disposed electronic assets

Records management

» Liability and the Certificate of Destruction

CASCADE ASSET MANAGEMENT

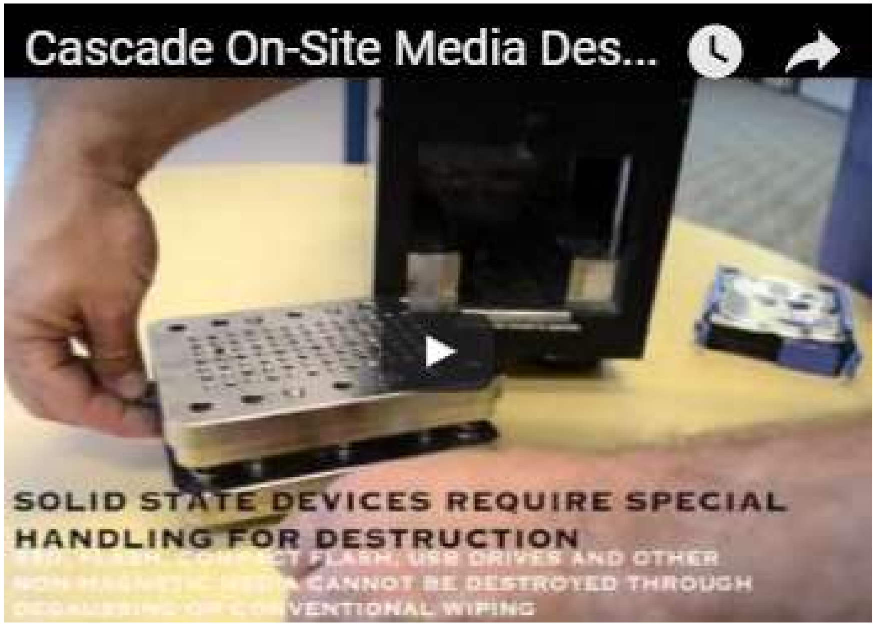
BrainStorm FOR ED TECHS, BY ED TECHS EDUCATIONAL TECHNOLOGY CONFERENCE 2019

Classification of sanitization methods

Clear: protection against a keyboard attack

Purge: protection against a laboratory attack

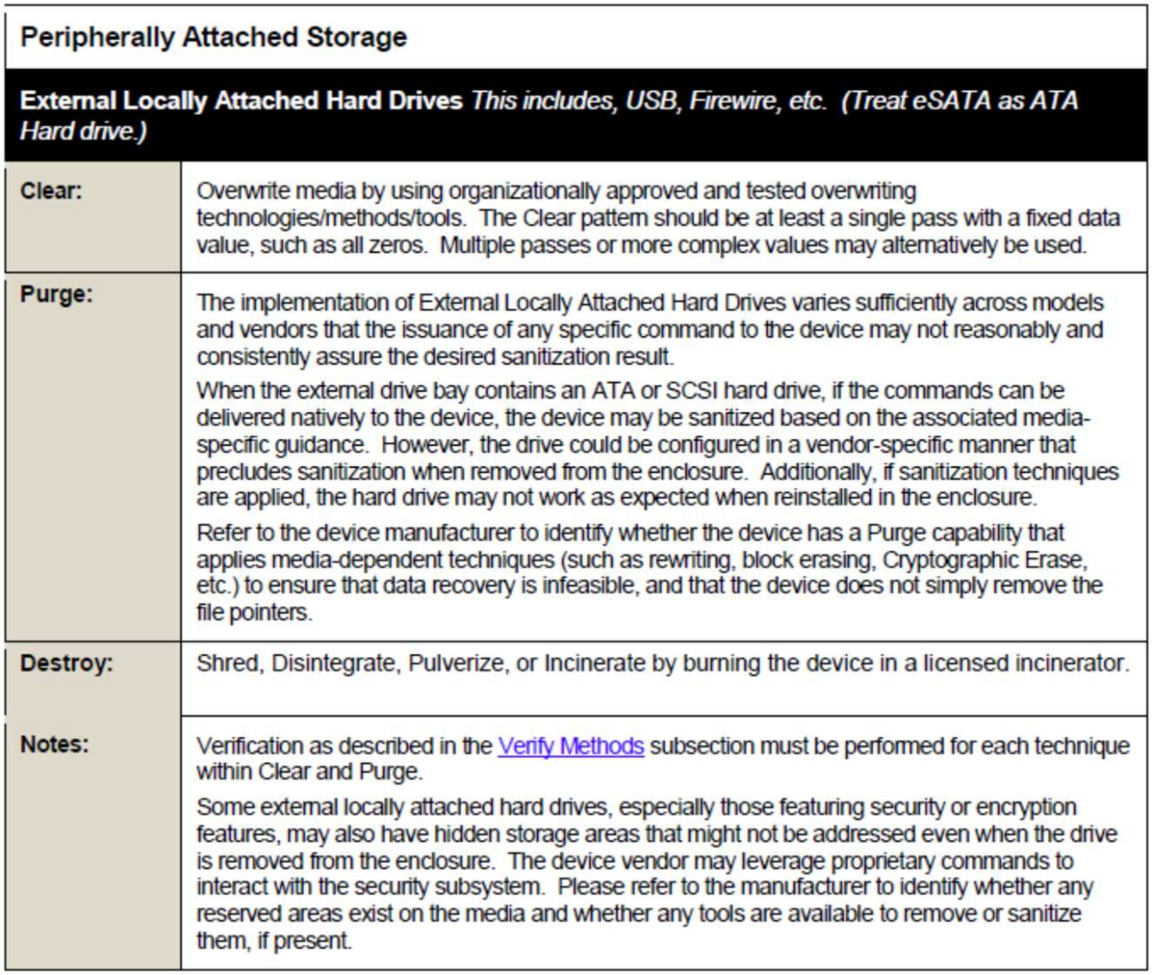
Destroy: media cannot be reused *(physical destruction)*



Cascade On-Site Media Des...

SOLID STATE DEVICES REQUIRE SPECIAL HANDLING FOR DESTRUCTION

SSD, FLASH, COMPACT FLASH, USB DRIVES AND OTHER NON-MAGNETIC MEDIA CANNOT BE DESTROYED THROUGH DEGAUSSING OR CONVENTIONAL WIPING



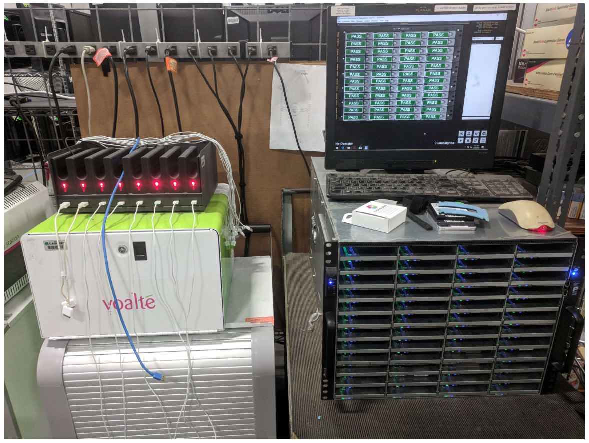
Peripherally Attached Storage	
External Locally Attached Hard Drives *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Example in NIST Guidelines of how to meet each sanitization level for a type of media.

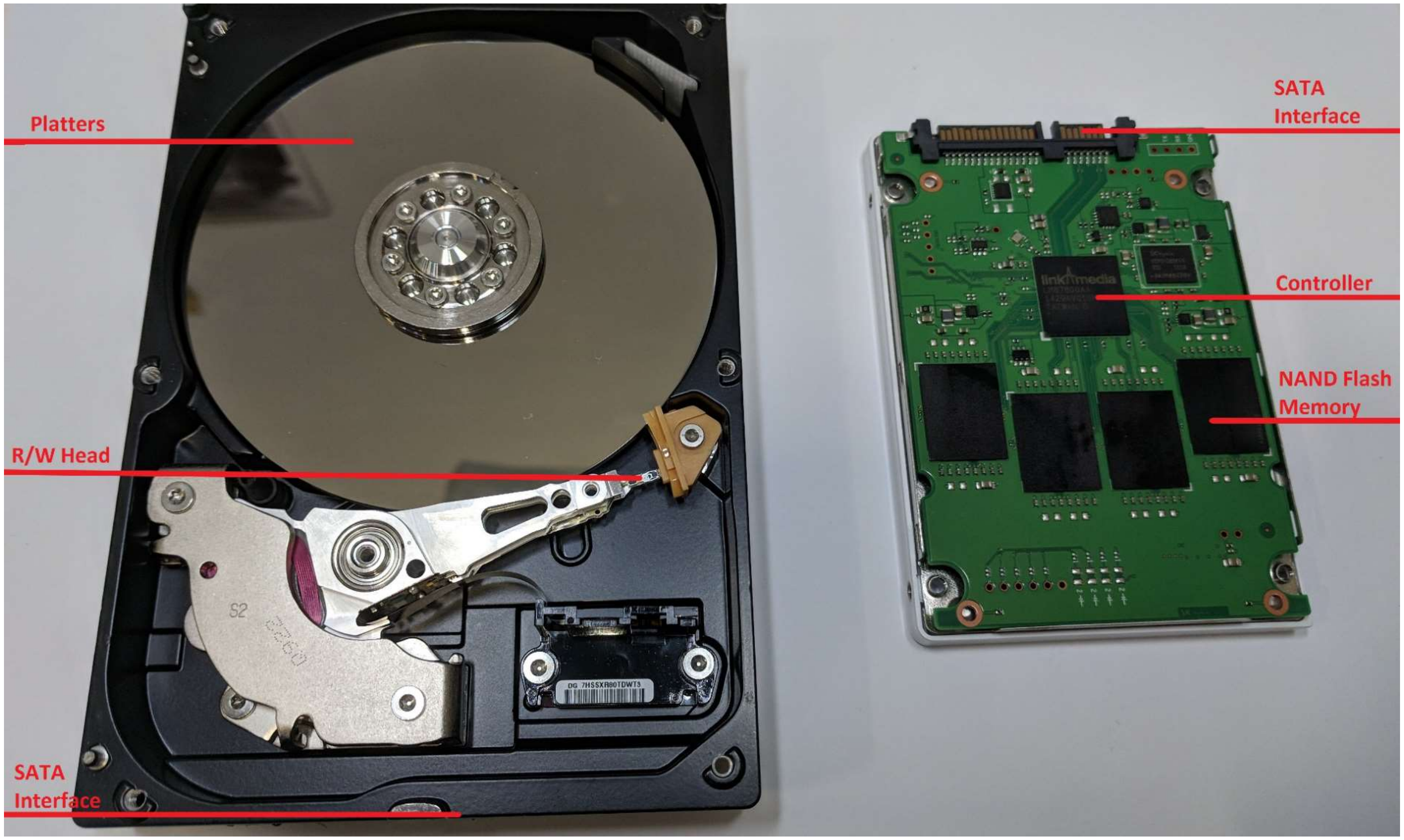
Increasing complexity of testing & sanitization

Sanitization is more complex with SSDs, mobile devices, enterprise equipment, increased customization, flash media, etc.

- Larger volumes of specialized testing required
- Requires higher level of knowledge & skill from technicians
- Additional hardware, software, and peripherals – flexible testing stations
- Increase in servers X increase in HDD storage = more capacity needed
- Testing requirements (e-Stewards, R2, NAID, etc)
- Licensing requirements



Increasing complexity of testing & sanitization



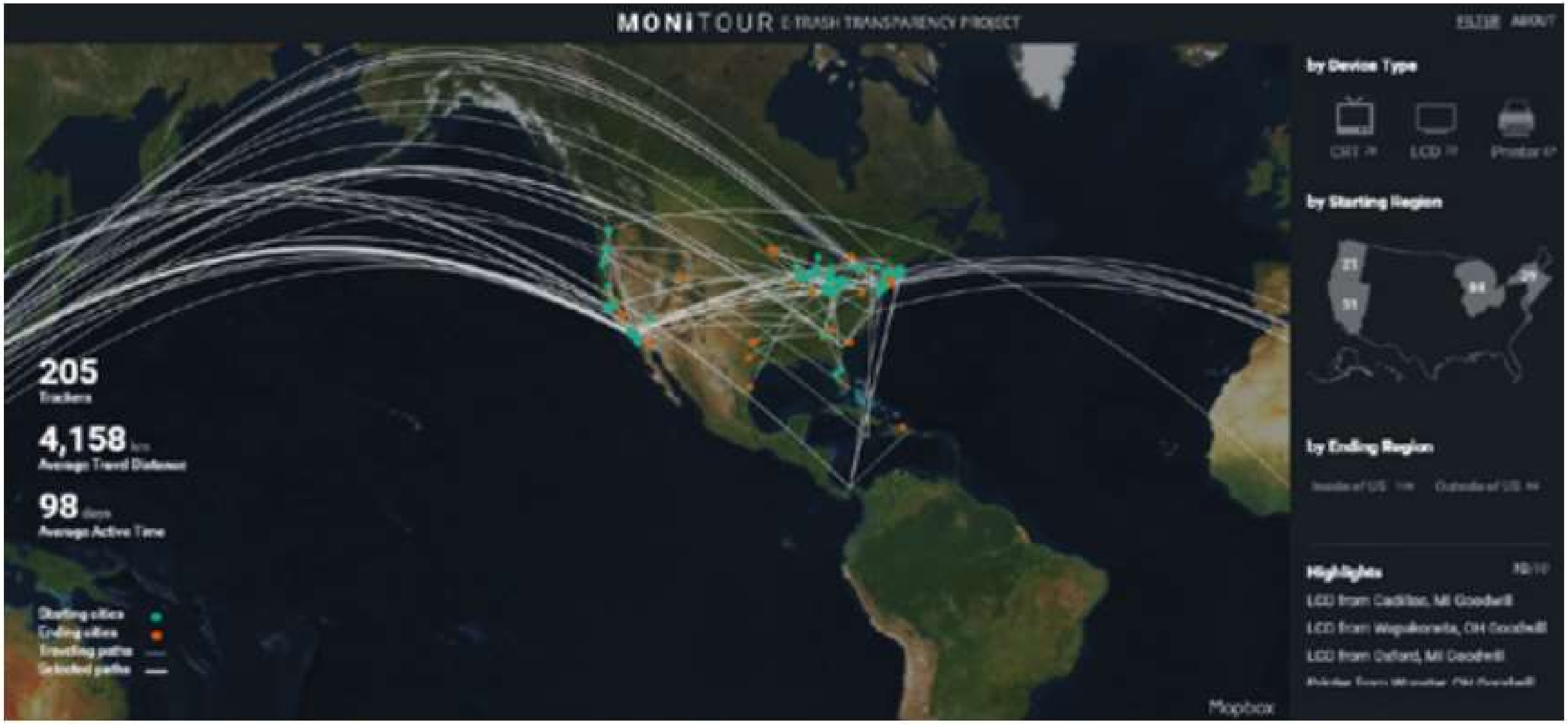
ITAD Vendor Due Diligence – Data Security

ITAD vendors should have:

- Employee screening
- Contracts
  - Indemnification
  - Subcontractor/service provider certifications
  - Transfer of custody
- Breach notification
- Employee training/written procedures
- Operational security specifications

A1

Environment: e-Waste Export



Monitour/e-Trash Transparency Project visualization created by MIT's Senseable City Laboratory, 2016, showing all of the export routes of the project. Note, the solid white band from the Northeast/Midwest part of the country, showing movement by rail to Long Beach/Los Angeles Port and then to Hong Kong.

Basel Action Network - http://www.ban.org

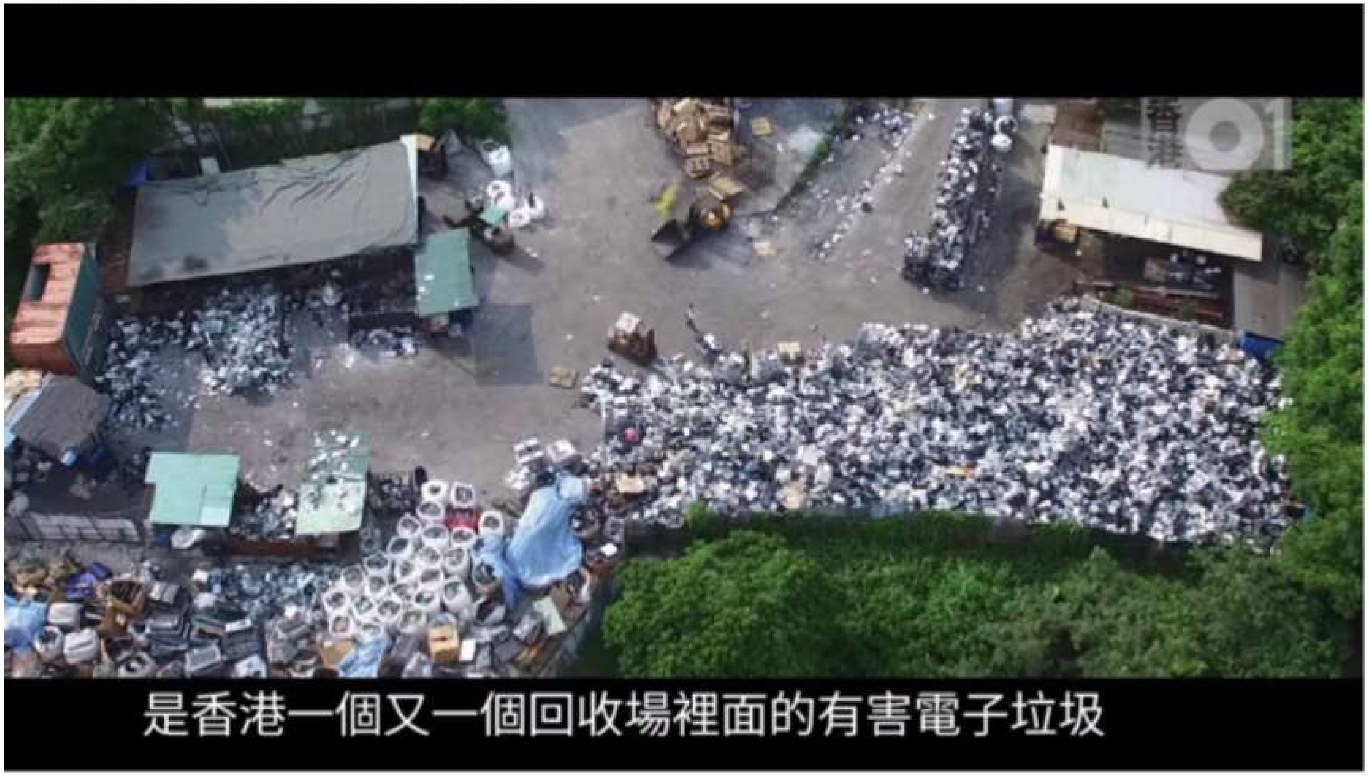
Slide 18

A1 40% of trackers dropped off at recyclers went overseas, 93% of those to developing countries

Author, 3/4/2019

Environment: e-Waste Export

HK01 News in Hong Kong, viewing electronics junkyards by use of drones. Screenshot.

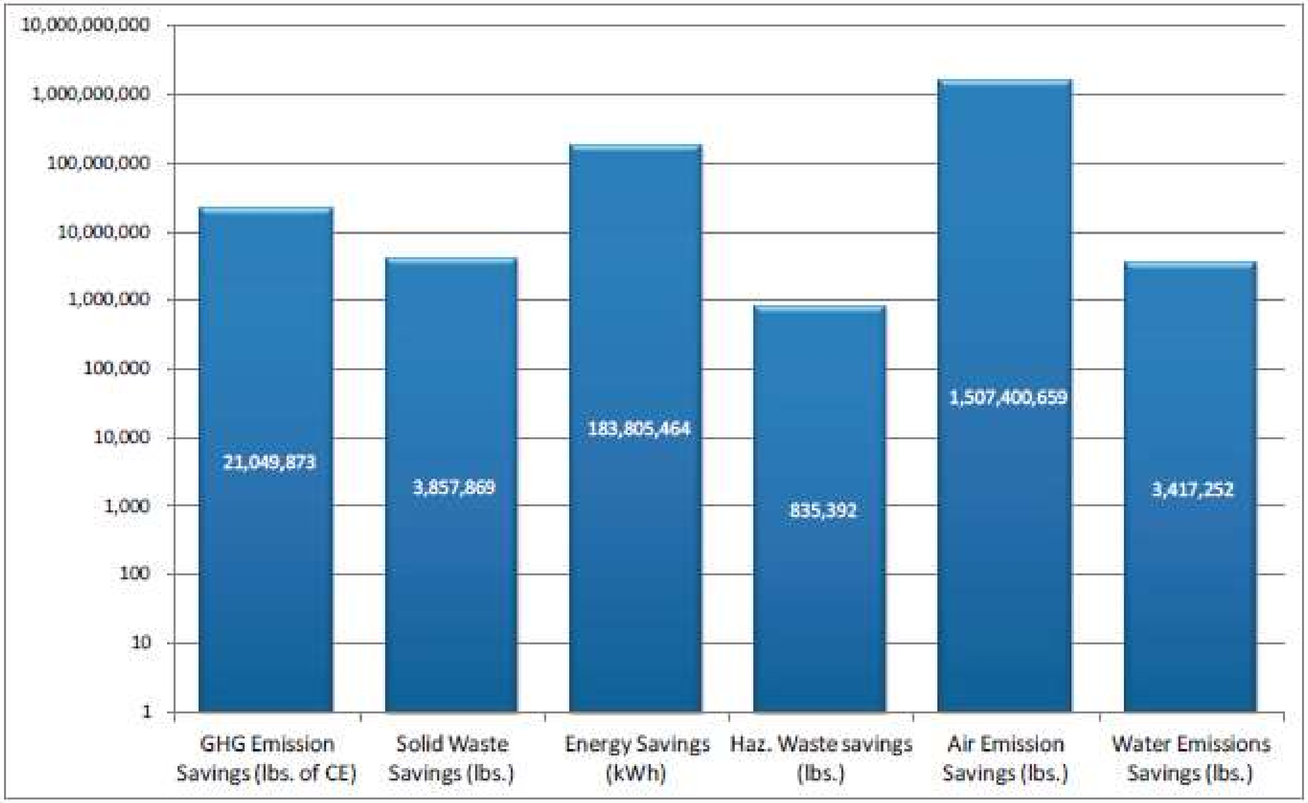


是香港一個又一個回收場裡面的有害電子垃圾

Basel Action Network - http://www.ban.org

Environment: Domestic Recycling Issues

Environment: Benefits



CASCADE ASSET MANAGEMENT

BrainStorm FOR ED TECHS, BY ED TECHS EDUCATIONAL TECHNOLOGY CONFERENCE 2019

Environment: Recycling Challenges

IFIXIT

ITAD Vendor Due Diligence - Environment

ITAD vendors should have:

- Downstream due diligence
- Permits
- Contracts
- Closure plan/insurance
- Material accounting methods (e.g. “mass balance”)
- Reused assets fully tested and sold with warranty

e-Stewards CERTIFIED

R2

Maximize Value

- Evaluate value with refresh rates
- Don’t destroy drives if you don’t have to
- Keep adapters, cables, batteries with retired assets; part out only what you need (memory, etc.)
- Work with an ITAD that does “break-fix” work
- Work with ITADs that have established resale markets for servers and networking equipment
- Consider donation programs – positive social impacts

EVERYONE MADISON
INTERNET ACCESS FOR ALL

Thank You!

TJ Barelmann
608-316-6634
tj@cascade-assets.com
cascade-assets.com

repair.org