IT Asset Disposition Trends and Best Practices

January 2016

This second annual benchmarking report provides information and research on security, environmental, and financial issues related to IT Asset Disposition (ITAD). It also includes an overview of the NIST Media Sanitization Guidelines and illustrates best practices in data destruction for a wide variety of storage media.

This report was built from data Cascade compiled through (1) a December 2015 customer survey, (2) an evaluation of more than 200,000 assets processed by Cascade in the past twelve months, and (3) a review of related industry research.

The ITAD industry is expected to confront serious obstacles in 2016. Diminished recycling scrap values, increased regulatory scrutiny, and pressures to reduce costs all threaten the ability for processors to operate successfully.

Despite these challenges, Cascade was able to demonstrate a **savings of 27.4%** in net costs for its clients last year. This accomplishment was due to more aggressive repair and refurbishment activities, which generated greater resale revenues. In addition, Cascade collaborated with clients on smart cost containment programs.

This report presents information and insights gained from research and experience to help more organizations reduce their ITAD costs while ensuring their security and environmental interests are protected.

Links to additional content

Throughout this report, look for the "graduation cap" to continue your education and learn more about the topic being discussed. The on-line version of this report includes clickable links to additional research and more in depth analysis. You can also access free templates, tools, and calculators to help you make the most of your ITAD program. The electronic report is posted at:

www.cascade-assets.com/2016report

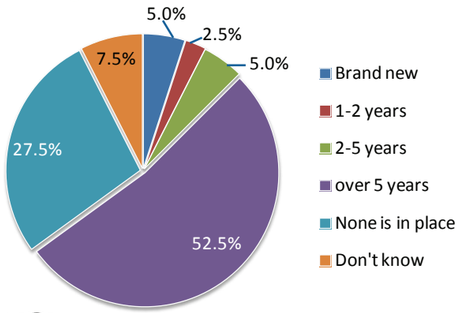
A report prepared by

Cascade Asset Management

Additional details and source material at www.cascade-assets.com/2016report
608-222-4800 * info@cascade-assets.com

IT Asset Management Programs

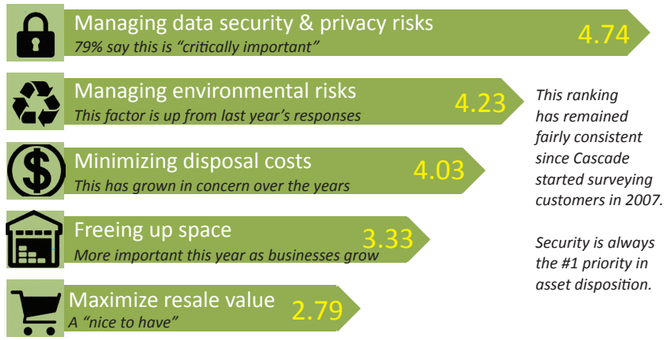
How long have you had an ITAM program in place?



Learn more about our survey respondents. Access demographic details.

How important are the following considerations when disposing of your surplus technology?

rated on a scale of "1 to 5" with 5 being "critically important" and 1 being "least important"



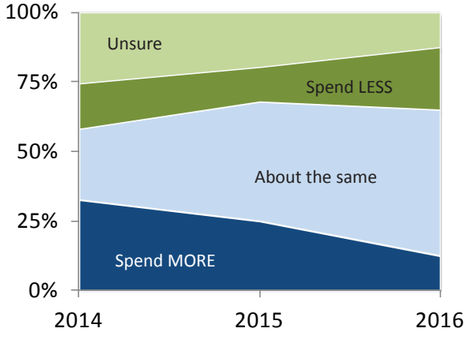
This ranking has remained fairly consistent since Cascade started surveying customers in 2007.

Security is always the #1 priority in asset disposition.

Effective IT asset retirement begins with a coordinated IT Asset Management process. Successful ITAM strategies help organizations **generate value** from their IT assets and **reduce risk**. The IT Asset Manager is responsible for managing the disposition vendor, ensuring personally identifiable information is destroyed, and reporting asset status for financial accounting. Cascade has found that the most effective ITAM programs involve stakeholders from IT, risk management, facilities, environmental health & safety, finance and procurement. Because the CIO and other executives of an organization can be personally liable for the improper disposition of IT assets and loss of data during disposal, it is a good idea to include them in the ITAM program, too.

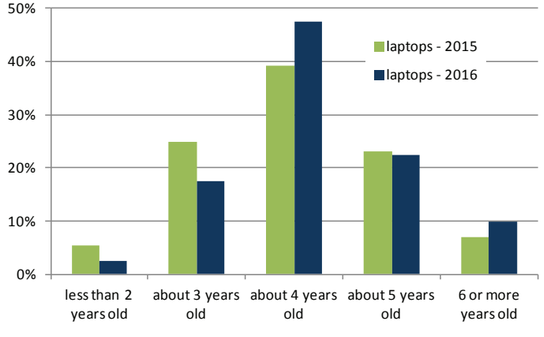
IT Asset Purchase and Disposition Forecast

Do you expect to spend more or less money on IT hardware next year?



There's been a significant decline in the expectation to spend more on IT hardware each year (from 32.7% in 2014 to 12.5% in 2016). As a result, IT asset managers are challenged to find ways to stretch their budgets.

How old are the majority of laptops you expect to retire in 2016 *(compared to 2015)*?



Survey respondents are planning to extend the refresh rates of their laptops and desktops hoping this will save costs. Cascade's report on minimizing TCO shows this may not be an effective cost cutting strategy and will cost companies more in the long run.

Read our article about why an extended refresh rate is not always a good way to reduce IT costs.

IT Asset Disposition Policies

Many industries are regulated by some type of Privacy Protection Rule such as HIPAA or FACTA. Firms are also audited to voluntary standards which require that the organization have a robust security policy and an effective program in place to destroy data on retired devices.

To be effective, security policies should address specific elements, such as employee training, vendor management, and data sanitization standards. A policy is an important tool for setting consistent standards throughout the organization. When enforced, the policy helps prevent data breaches and demonstrates the organization took reasonable precautions to prevent a loss of data. In 2016, the US Health and Human Services Office of Civil Rights will be auditing healthcare providers and will be looking for evidence of a policy.

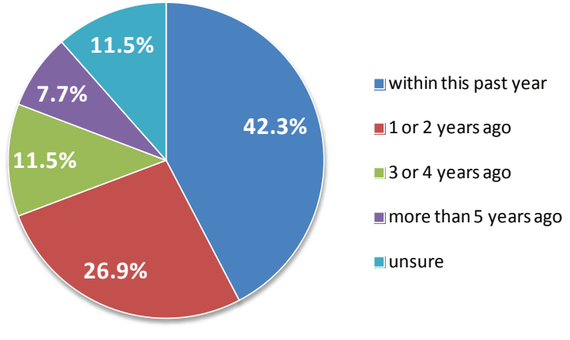
If you have a policy, what types of assets are included?

- personal computers 100%
- laptops 92.3%
- servers and related 96.2%
- mobile devices 69.2%
- print devices 61.5%

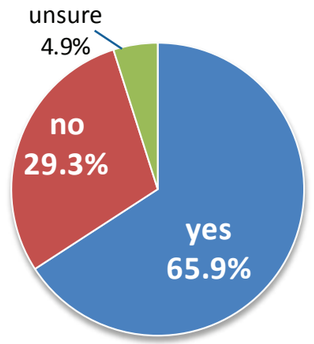
Most security regulations require security policies be "reviewed and updated as needed," which typically means they should be checked annually. Be sure to conduct a threat assessment against your current asset base to ensure data protection and destruction programs are current and effective.

Download our free Data Security Template and learn more about this year's HIPAA Phase 2 audits.

When was the last time your policy was reviewed or updated?



Does your organization have a policy that addresses how IT assets are disposed?



What aspects of IT asset disposition do your policy address?

- ☑ Employee training. 7.7%
- ☑ Data destruction on employee mobile devices (BYOD issues) 11.5%
- ☑ Sale of equipment to employees. 26.9%
- ☑ Employee acknowledgment of policy . . 34.6%
- ☑ Re-purposing assets internally. 42.3%
- ☑ Company-owned mobile devices 50.0%
- ☑ Specifying a wiping standard for the sanitization of assets 57.7%
- ☑ Disposition of assets to 3rd party (such as Cascade) 88.5%

Every item on the clipboard should be included in a company's data security policy and program. Most importantly, employees are expected to be informed and trained on the policy. Keeping a signed acknowledgment of the policy on file is the best way to demonstrate to auditors that you took reasonable efforts to train staff, which will prevent compliance fines and should also mitigate potential data breaches.

CASCADE ASSET MANAGEMENT

Additional details and source material at www.cascade-assets.com/2016report
608-222-4800 * info@cascade-assets.com

Data Destruction Methodologies

The NIST 800-88 Guidelines for Media Sanitization provide a comprehensive approach to identifying data storage devices and eliminating data from these devices. Here's what it covers.

Types of sanitization methods in NIST

The Guidelines establish three levels of data destruction that can be applied to different data storage devices. Organizations should pick the physical destruction of electronic sanitization method that meets their tolerance for risk. The destruction method may be different for each class of storage devices.

Clear is the method that uses software or hardware products to overwrite user-addressable storage space on media with non-sensitive data, when available. This is done by writing "0's or 1's" over all sectors in a drive or storage device. If this isn't possible (such as in a basic cell phone or piece of office equipment), manufacturer resets and procedures that do not include rewriting might be the only option to **Clear** the device. Items that are **Cleared** may be able to be reused after they are sanitized.

Purge may be an overwrite, block erase, or Cryptographic Erase through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the typical read and write commands. Items that are **Purged** may be able to be reused after they are sanitized.

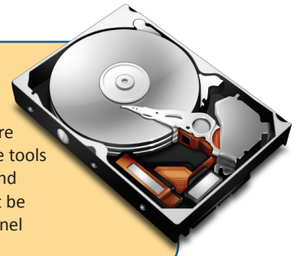
Destroy is a physical process that makes data retrieval infeasible using state of the art laboratory techniques. **Destruction** methods include shredding, incineration, melting and pulverizing. Degaussing is also considered a destruction technique when used properly. Bending, cutting and drilling holes through a storage device are NOT considered destruction techniques. **Destroyed** items are not able to be reused. Demanufacturing followed by shredding or smelting is Cascade's method for physical destruction.

Read the NIST 800-88 Guidelines and related background information.

Using the NIST Guidelines to establish your information destruction program

The scope of the NIST Media Sanitization Guidelines is much more expansive than what was included in the legacy DoD data wiping standard. The Guidelines address how to set up a comprehensive system for creating policies, assigning responsibilities, determining risk tolerances, and informing decisions to sanitize or destroy data on a wide variety of media and devices. A short summary of applicable sanitization methods for various products is provided here.

Hard Drives using Magnetic Media Storage



Includes ATA, SCSI and Fibre Channel drives

A one-pass overwrite meets the **Clear** requirement; Secure Erase, Cryptographic Erase, or other embedded overwrite tools meet the **Purge** requirement; Shredding, disintegrating and burning meet the **Destroy** requirement. Verification must be performed for each **Clear** or **Purge** technique. Fibre Channel drives require specialized sanitization.

Mobile Devices with Flash Memory

Includes smart phones and tablets

Clear or **Purge** can generally be achieved by resetting to factory settings and/or selecting a full sanitize ("Erase All Content") option. Each manufacturer and Operating System requires a unique sanitization process. **Destroy** by shredding (remove batteries first!) - Ensure SIM cards are removed and destroyed as well.

Flash Memory-Based Storage Devices

Includes Solid State Drives (SSDs), USB drives, SD cards, and embedded flash memory on boards

Clear may be achieved using ***validated*** overwriting tools and may require one or two pass sanitization. Some flash memory can be **Cleared** by resetting to factory state. **Purge** can be achieved on some devices with Block Erase or Cryptographic Erase features - but verification is required of each **Purge**. Each manufacturer has different sanitization requirements. Because these devices use chips and are small, the **Destroy** specification can only be met by running pins through chips, fine shredding, pulverizing and/or melting.

Office Equipment

Includes copiers, printers, and multifunction machines

These devices may contain flash memory or magnetic hard drives. **Clear** can generally be achieved by resetting to factory settings. **Purge** may be applicable to specific devices and is dependent on the firmware of the device. Units with removable storage media can follow the sanitization technique for the associated storage device. **Destroy** these devices by removing any storage media and shredding. The whole unit does not necessarily need to be shredded.

What about the Department of Defense Standard?

The DoD 5220-22.M 3-pass wipe standard was originally published in 1995 in the National Industrial Security Program Operating Manual (NISPOM). In 2007, the Defense Security Service updated its "Clearing and Sanitization Matrix" and said, "DSS will no longer approve overwriting procedures for the sanitization or downgrading of IS storage devices." The NIST Guidelines, originally published in 2006 and updated in 2014, are seen as a replacement to the legacy DoD standard.

Download our White Paper "Debunking the 3-pass overwrite requirement."

Hard Copy Storage

Includes paper and microforms

Clear and **Purge** are not possible sanitization methods for these media. To **Destroy**, paper must be shredded using a cross cut process into particles 1mm x 5mm in size or smaller. Paper may also be pulverized through a 2.4mm screen. Microforms (microfilm, microfiche or photo negatives) are considered destroyed when burnt to a white ash.

Magnetic Media and Optical Media

Includes tape drives, floppies, CDs, and DVDs.

Clear and **Purge** are not possible sanitization methods for CDs or DVDs. Magnetic Media (tapes and floppies) can be **Cleared** through a one-pass overwrite and verification or can be **Purged** using a proper degausser. These media meet the **Destroy** method through incineration or shredding.

Networking Devices

Includes routers and switches

Routers and switches may contain IP addresses and other identifiable information that can facilitate hacking into a network. The **Clear** method of sanitization involves performing a full manufacturer's reset back to default factory settings. **Purge** may be available on some devices using block erasing. **Destroy** is achieved through shredding.

CASCADE ASSET MANAGEMENT

Additional details and source material at www.cascade-assets.com/2016report
608-222-4800 * info@cascade-assets.com

Security Concerns

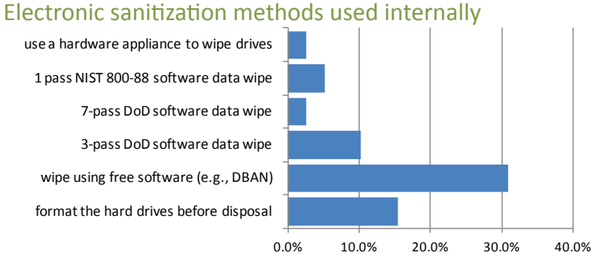
Which methods do you use (internally) to control and destroy data on hard drives?

Organizations report that they may use one or more ways to control and destroy data on their hard drives before these devices leave their premises. Interestingly, a significant number (43.6%) report they do not use any internal controls on their hard drives. Instead, they rely on Cascade as their asset disposition partner to perform all data destruction on their behalf.

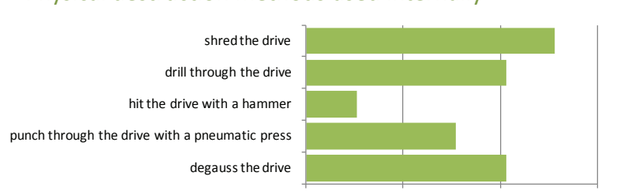
Cascade recommends all organizations adopt appropriate methods of media destruction based on the NIST 800-88 Guidelines for Media Sanitization and consistent with their tolerance for risk. In addition, actively tracking assets through tools like Computrace/Absolute DDS contributes to a more secure chain of custody of assets through final disposition. Cascade helps companies de-activate Computrace enabled devices as part of the disposition process.

Read Cascade's article about encryption and Computrace controls.

Electronic sanitization methods used internally



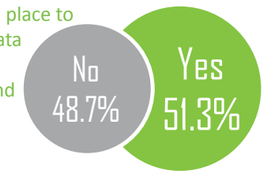
Physical destruction methods used internally



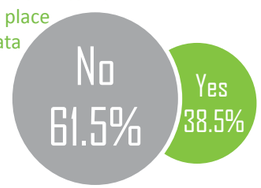
Special media sanitization

Different technologies are required to destroy data on Solid State Devices (SSD) and flash media in many tablets and smart phones. Our survey indicates many firms are still looking for processes to sanitize these media and responses are virtually identical to last year's survey.

Do you have an internal process in place to destroy data on smart phones and tablets?



Do you have an internal process in place to clear data on SSDs prior to disposal?



Data breach incidents - something to avoid!

There are now plenty of examples to justify investments in security controls and disposition programs. Increased penalties and regulations require organizations to implement ITAD strategies that seek to prevent and limit the loss of consumer and patient data.

Financial Sector

In 2015 there were 9 security related enforcement actions by the FTC. Also, the US Court of Appeals confirmed the FTC's authority to protect consumer data (upholding a challenge by Wyndham Worldwide). On June 30, 2015, the FTC announced its new "Start with Security" education initiative, which encourages businesses to protect data on devices taken out of service.

HIPAA phase 2 audits in 2016

The Office of Civil Rights is set to begin conducting desk and on-site audits of approximately 350 Covered Entities (including health care providers, health plans, and health care clearinghouses) in early 2016. The scope of the audits is published on the HHS web site.

Healthcare breaches

In 2015, over 113 million patients were impacted by data breaches at 254 Covered Entities (as reported to HHS). There was a huge increase in hacking incidents (10 times more people affected in 2015 vs. 2014). Breaches from improper disposal (affected 76,226 people in 2015) and loss/theft (affected 749,502 people) are still significant.

Cost of breach

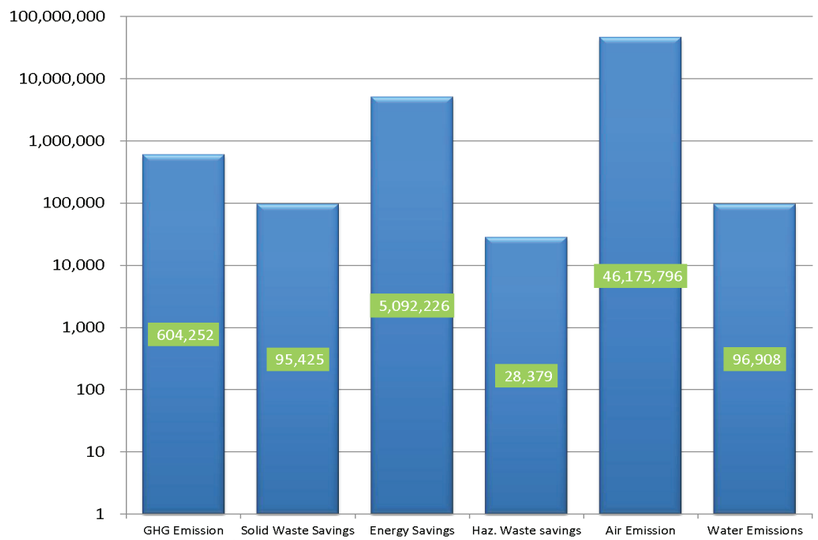
According to the Ponemon Institute, the average cost of a data breach increased 23% over the past two years to $3.79 million. The average cost paid for each lost or stolen record containing sensitive data increased 6% to $154.

See a list of published data breaches and compliance actions related to data security.

Environmental Issues

Environmental benefits of electronics reuse and recycling by Cascade

IT equipment received from all customers between December 2014 to November 2015



The reuse and recycling of electronics by Cascade and its customers had the equivalent environmental impact of . . .

- saving enough energy to power 15,406 typical U.S. homes
- removing 6,463 passenger cars from the road for 1 year
- keeping 10,610 tons of carbon out of the atmosphere

Calculate your own environmental impact of electronics reuse and recycling.

Illegal disposal now attracting regulators

There were a number of prominent cases in 2015 involving civil and criminal penalties against businesses engaged in the illegal dumping of e-waste. Expect more incidents in 2016.

2,500 tons of CRTs — Apr 16, 2015 - A Minnesota based e-scrap firm was fined $125,000 for storing 2,500 tons of CRT glass in more than 100 semi trailers around the Twin Cities. The company eventually closed its doors in May.

30 feet wide — Oct 15, 2015 - A Kentucky recycler admitted to dumping hundreds of pallets and dozens of boxes filled with TV monitors in a hole roughly 10 feet deep and 30 feet in diameter 100 yards from their facility.

$26 million — Dec 15, 2015 - California reaches $26 million settlement with **Comcast** for unlawfully disposing of electronics. The State had previously cited AT&T for similar violations.

Learn more about the recycling markets and how to protect yourself from unscrupulous processors.

Low recycling values create challenges

While the U.S. economy may seem to be humming along, the value of scrap metals harvested from electronics has dropped dramatically from its peak in 2011. This is due to slower economic growth in China and Europe, a strong dollar valuation, and a glut of copper, aluminum and precious metals on the market.

At the same time, the costs for handling the hazardous materials in electronics are increasing. Compliance costs and the lack of markets for leaded glass and mercury products make it more difficult and costly to find good homes for these materials.

It is expected that the situation won't get any better through 2016.

Commodity price declines from 2011 to 2015

Copper *down 69%*

Gold *down 36%*

Iron *down 71%*

CASCADE ASSET MANAGEMENT

Additional details and source material at www.cascade-assets.com/2016report
608-222-4800 * info@cascade-assets.com

Maximizing Value

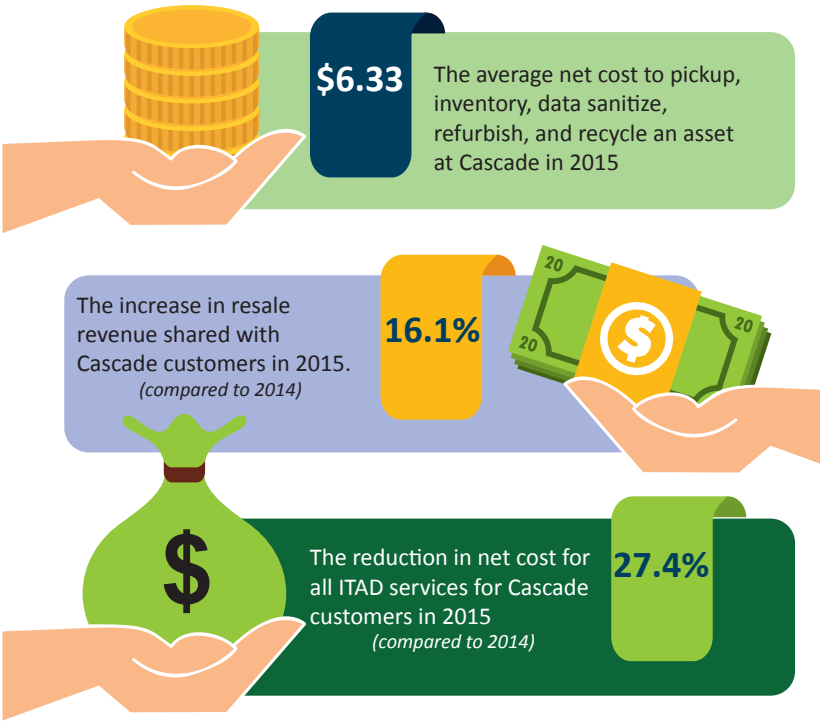
Cascade data analysis - 2015 ITAD costs

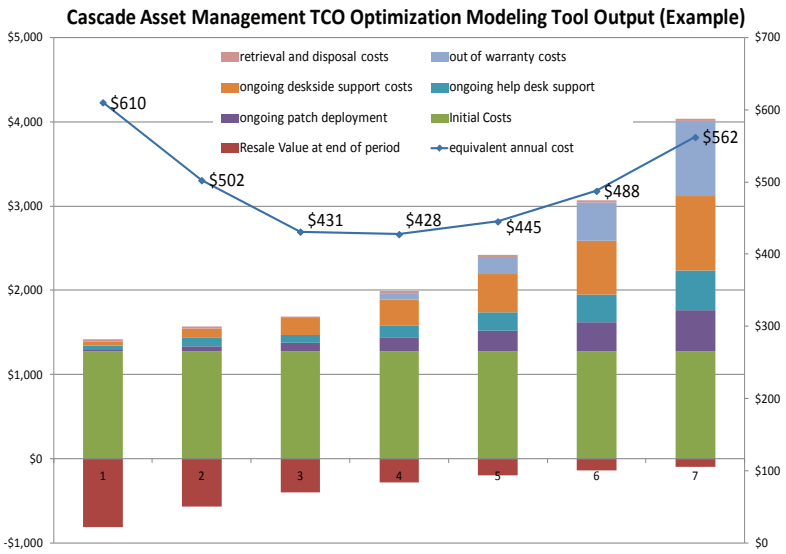
One of the biggest complaints with IT Asset Disposition programs is the cost. So how much does it cost to outsource ITAD services to a professional ITAD firm? For Cascade, the cost is dependent on what value added services you select and whether these costs can be offset by revenues generated from the resale of equipment.

While your disposal policy should dictate your security and environmental processing requirements, there are steps every organization can take to reduce disposition costs or turn this process into a revenue generator.

Companies that maintain a regular 3-4 year refresh program, allow for the resale of reusable equipment, and maintain their equipment while in use, will generally see most (if not all) of their disposition costs covered by revenue offsets.

See more detail about how Cascade reduced our customers' net ITAD costs by 27.4% in 2015.





Maximizing asset value through its lifecycle

The best way to optimize the value of your IT assets is to consider their entire life cycle benefits and costs.

First, understand the value the assets provide to your organization, employees and customers. When IT assets are productive and well suited for their role, they demonstrate a positive impact.

Then, identify the costs to purchase, maintain and dispose of those assets. The value generated from the resale of working excess assets helps to offset these costs.

Taken together, you can determine the optimal refresh rate that results in the lowest average annual cost for your IT assets.

Determine the optimal refresh rate for your assets by using Cascade's TCO modeling tool.

Contact Cascade for further assistance.

Safe & Sound® IT Asset Retirement Since 1999.

Learn about Services

www.cascade-assets.com/solutions
info@cascade-assets.com
608.316.1606

Schedule a Pick-up

www.cascade-assets.com/pickup
pickup@cascade-assets.com
608.222.4800

"Cascade Asset Management is an affordable, efficient and secure way to rid your work site of unwanted and/or obsolete IT assets. The customer service was very good and the pickup process was fast and easy. Highly recommended."

- Lucas Weaver, Aerovex Systems

CASCADE ASSET MANAGEMENT