SEM®

Classified and High Security Data Destruction

MEDIA SANITIZATION

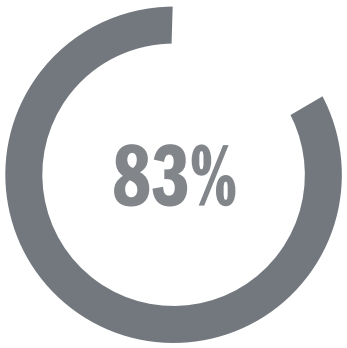
Best Practices for Organizations

IT TAKES 20 YEARS TO BUILD A REPUTATION AND A FEW MINUTES OF CYBER-INCIDENT TO RUIN IT.

– STĒPHANE NAPPO

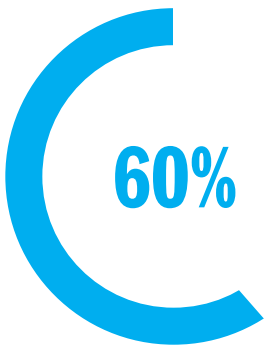
CYBERSECURITY STATS

IBM Security and Ponemon Institutes' The Cost of a Data Breach Report offers IT, risk management and security leaders a lens into factors that can increase or help mitigate the rising cost of data breaches. This research studied 550 organizations impacted by data breaches. The breaches occurred across 17 countries and regions and in 17 different industries. Key stats:



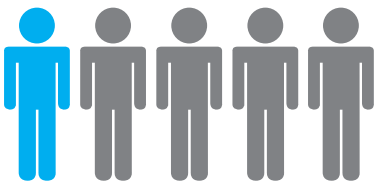
RISK IS EVERYWHERE

83% of organizations studied have had more than one data breach.



BREACHES AND LEAKS ARE EXPENSIVE

60% of organizations' breaches led to increases in prices passed on to customers.



THIRD-PARTY RISK IS REAL

One in five breaches occurred because of a compromise at a business partner.

REACHING AN ALL-TIME HIGH, THE COST OF A DATA BREACH AVERAGED USD 4.35 MILLION IN 2022. THE UNITED STATES HAD THE HIGHEST AVERAGE TOTAL COST OF A DATA BREACH AT USD 9.44 MILLION.

DETERMINING RISK

IS THERE A STATUTE OF LIMITATIONS ON BREACH FROM END-OF-LIFE MEDIA?

NO.

It is really that simple. If a discarded or recycled drive or device is involved in a breach 5, 10, or 20 years down the road, the originating organization is still responsible. Because so many drives and devices end up in highly targeted and highly pilferable landfills and trash heaps, this lack of a statute of limitations is concerning.

End-of-life data destruction isn't just good sense for the present; it also makes sense for the future.

As technology evolves, so do ways in which cybercriminals and nefarious organizations or individuals can access data. Organizations typically prioritize active and resting data security protocols such as firewalls, threat detection, etc., but pay little attention to end-of-life data — a risky practice. Media sanitization should also be prioritized, and the cost to do so is comparitively minimal.

SECURITY STANDARDS

THE FIRST QUESTION WHEN IT COMES TO INFORMATION END-OF-LIFE SECURITY IS OFTEN, "WHAT IS REQUIRED?"

DIN 66399 standards are internationally recognized; however, DIN standards are also subjective in nature, with the organization housing the data being sole determiner of the data's security level.

NIST 800-88 is highly adopted in the United states, but it also only provides guidelines and suggestions rather than a clear path to end-of-life security. The reality is that unless you are destroying to NSA mandates — globally considered the golden standard — you will have risk. The level of acceptable risk is up to you.

BEST PRACTICE IN END-OF-LIFE MEDIA SANITIZATION

The protection of end-of-life information is far simpler than protection of active data. While active data requires firewalls, security protocols, encryption, and a myriad of other highly technical — and expensive — methodologies, protecting end-of-life data is relatively simple: destroy the data. How this is accomplished is where things can get tricky.

We've determined that DIN 66399 and NIST 800-88 standards are subjective and vague — so where does that leave us for end-of-life information security?

THE UNITED STATES NATIONAL SECURITY AGENCY

For classified and top secret information, the National Security Agency (NSA) determines the appropriate data destruction methodology and evaluates equipment for this purpose. While this may seem extreme to commercial organizations, the fact remains that all other end-of-life security protocols are subjective and open-ended.

The NSA's requirements for end-of-life media sanitization ensure that any and all data will be absolutely unrecoverable, even if subjected to sophisticated data recovery techniques. The price of NSA evaluated and listed equipment really is comparable to equipment that is only suitable for DIN 66399 or NIST 800-88 destruction.

SO WHY DON'T ORGANIZATIONS GO STRAIGHT FOR NSA LISTED EQUIPMENT? SIMPLE: BECAUSE THEY DON'T KNOW THAT THEY SHOULD.

NSA LISTED DATA DESTRUCTION EQUIPMENT

WHAT IT IS, WHERE YOU CAN FIND IT, AND WHAT YOU SHOULD LOOK FOR.

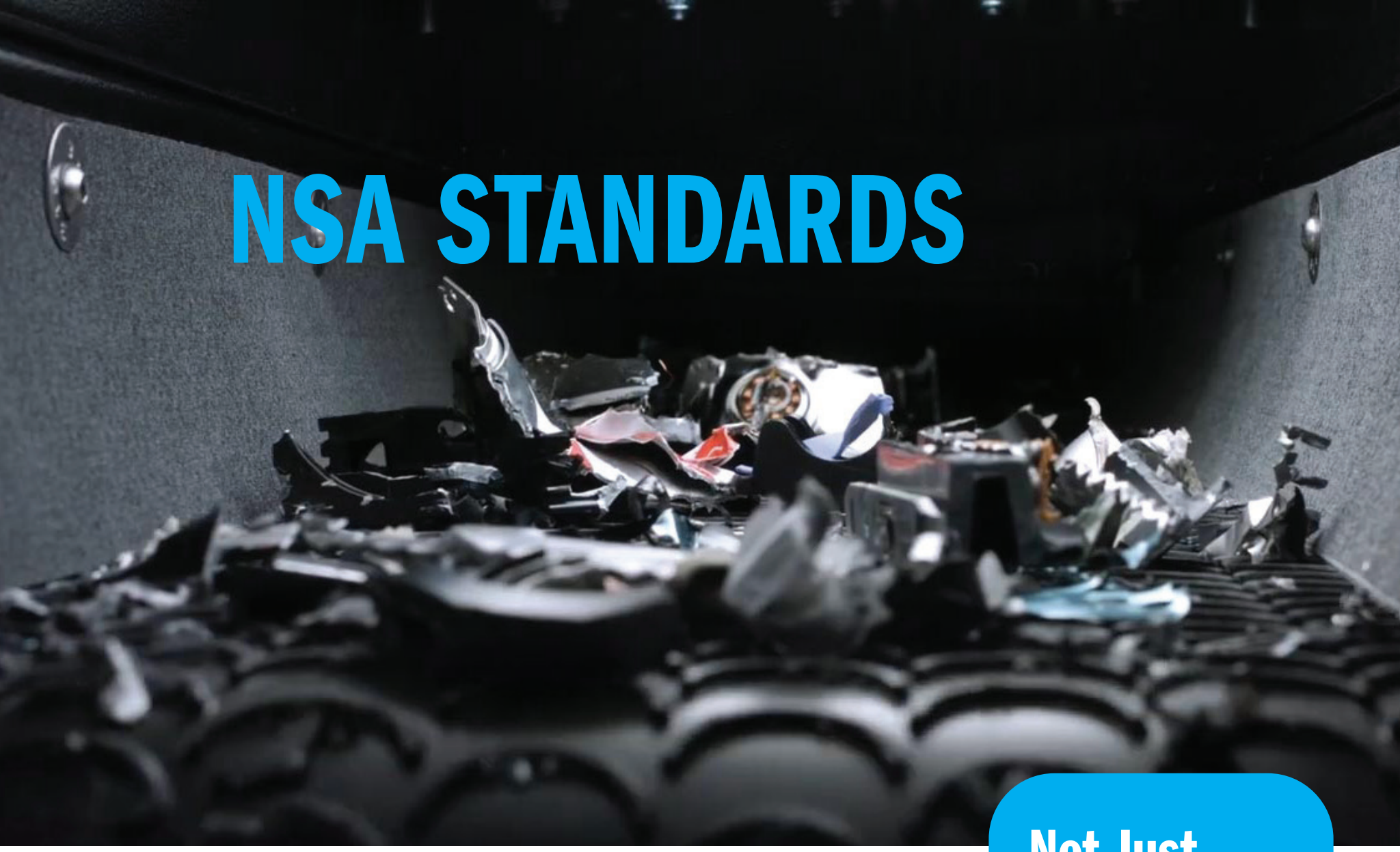
NSA evaluated equipment is just that: devices that have been rigorously tested and approved by the NSA to meet their stringent security requirements for destruction of end-of-life media. This testing includes determination that the final particle produced is consistent with the NSA's requirement. The NSA's evaluation also includes a 1-hour durability test that ensures the device can run and meet the mandated particle size for a solid hour without jamming or overheating.

The NSA maintains a list of evaluated equipment for each type of media requiring end-of-life sanitization. These lists can be found on the NSA's website and are updated frequently. Scan the QR code below for up-to-date lists:

< NSA Evaluated Products Lists

In addition to choosing a device that has been evaluated and listed by the NSA for data destruction, it is also imperative to find machinery that is manufactured with solid steel parts, as anything other than solid steel has the tendency to snap or warp under pressure. Data destruction devices endure massive pressure and wear, so choosing a device that incorporates superior technology and craftsmanship is a must.

Additionally, any NSA evaluated machine should come with a generous factory warranty that covers all parts for a minimum of one year.



NSA STANDARDS

HDDs AND MAGNETIC MEDIA

Rotational hard disk drives and magnetic media such as floppy disks and data tapes must follow a two-step process: degauss in an NSA listed degausser (minimum 20,000 gauss, or 2.0 Tesla), then physically destroy using an NSA listed crusher or any shredder/disintegrator.

SSDs AND eMEDIA

As they cannot be degaussed, SSDs and eMedia must be physically destroyed to a 2mm particle.

OPTICAL MEDIA

This is where things get tricky. CDs must be destroyed to a 5mm particle. Because they are denser, DVDs and Blu-ray Discs (BDs) must be destroyed to a 2mm particle.

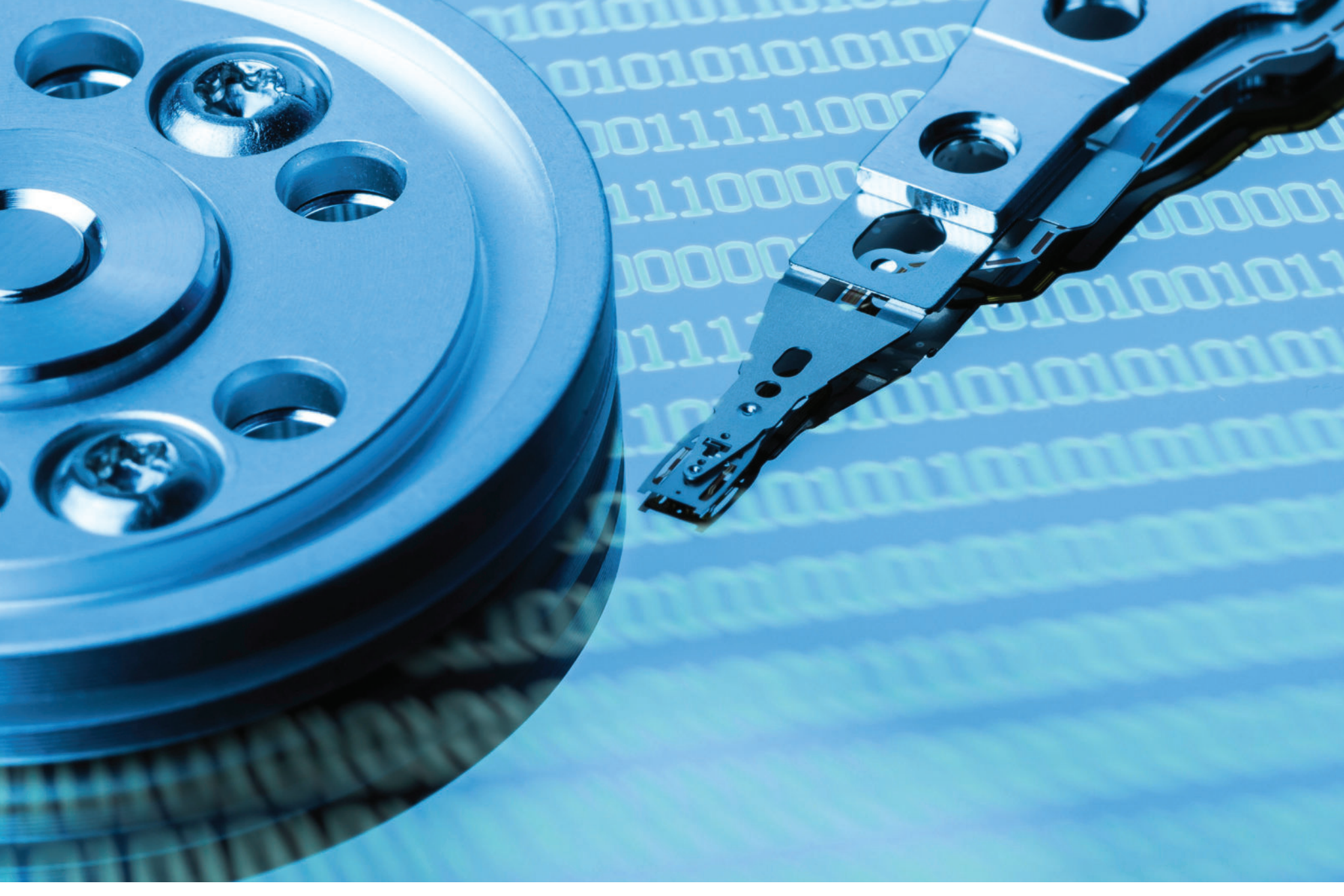
PAPER

Paper must be destroyed to a 1mm x 5mm maximum particle size. NIST 800-88 also follows this protocol.

Not Just Government

Cloud service providers, data centers, colos, and other commercial security-centric organizations also follow NSA standards for end-of-life media sanitization.

In fact, the Australian government also follows NSA standards for its own government data. The NSA has long set the precedent for best practices in media sanitization.



WHAT'S MY MEDIA?

Now that you know how to destroy media to NSA specifications, we want to make sure you know what type of media falls into which category.

There are six basic media categories that encompass all types of data-bearing media. Since there are so many different types of material that can contain high security, sensitive, or personally identifiable information (PII), figuring out which category your media falls into can be a challenge.

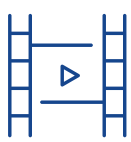
On the next page, we've broken down each category into its major components. This can be useful for determining which destruction mandate and associated device should be used for end-of-life data destruction.

MEDIA TYPES

Media is typically broken down into six major categories, which cover nearly all data-bearing devices at this time.

PAPER

Paper as well as printing plates and tipping foil used by commercial printers.

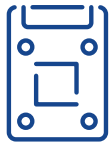


FILM

Micro-film, microfiche, slides, medical imaging, printer's film, and other film products

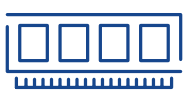
MAGNETIC

Floppy discs, ID cards, magnetic tapes, cassettes, credit cards, SIM cards



ROTATIONAL

Hard drives from computers, laptops, external devices, and data centers



E-MEDIA/SSD

Solid state drives, memory sticks, thumb drives, mobile phones, tablets, microchips, RFIDs

OPTICAL

Compact Discs (CDs). Digital Video Discs (DVDs), and Blu-ray Discs (BDs)

DESTRUCTION TYPES

01 DEGAUSSING

Degaussing is a process that creates powerful magnetic fields to sanitize magnetic storage media, rendering the drive useless. Degaussable media includes rotational hard drives; computer, audio, and video tapes; and magnetic removable storage media such as floppy, ZIP, JAZZ, REV, and Syquest disks.

02 CRUSHING

Crushing is the act of deforming a drive or device to make it unusable. The most common type of crusher uses a conical punch to pierce rotational hard drives. Additionally, SEM has created proprietary SSD crushers that utilize toothed rotors to pierce and crush even the tiniest microchips.

03 SHREDDING

Shredders incorporate toothed cutting blades that tear media to a specific particle size. High security paper shredders cross-cut to 2mm, while HDD shredders tear hard drives to a 38mm particle. Shredding is appropriate for paper, hard drives, optical media, film, license plates, and credit cards, to name a few.

04 DISINTEGRATING

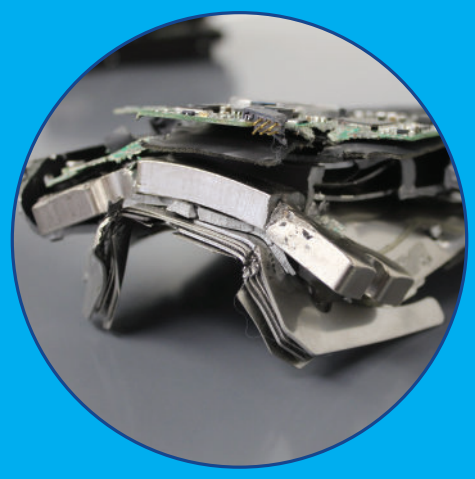
Disintegrators utilize stationary and rotating blades that continuously cut material to a size small enough to fit through a screen that is determined by the media being destroyed. Disintegrators destroying classified and high security solid state drives or paper are equipped with a 2mm screen, while those destroying less sensitive data may use a larger screen.

EXAMPLES

BELOW ARE SOME VISUAL SAMPLES OF SHRED SIZES FOR EACH OF THE TYPES OF DESTRUCTION:

DEGAUSS

While degaussing sanitizes all data on a drive, there is no visual confirmation. For this reason, the NSA requires classified drives to be physically destroyed after degaussing. Security-centric commercial organizations also follow this best practice.



CRUSH

Shown is a hard drive (HDD) crushed in an SEM 0101 hard drive crusher. The 0101 is capable of crushing all types of hard drives including enterprise drives, glass drives, laptop drives, server drives, and data center drives.

SHRED

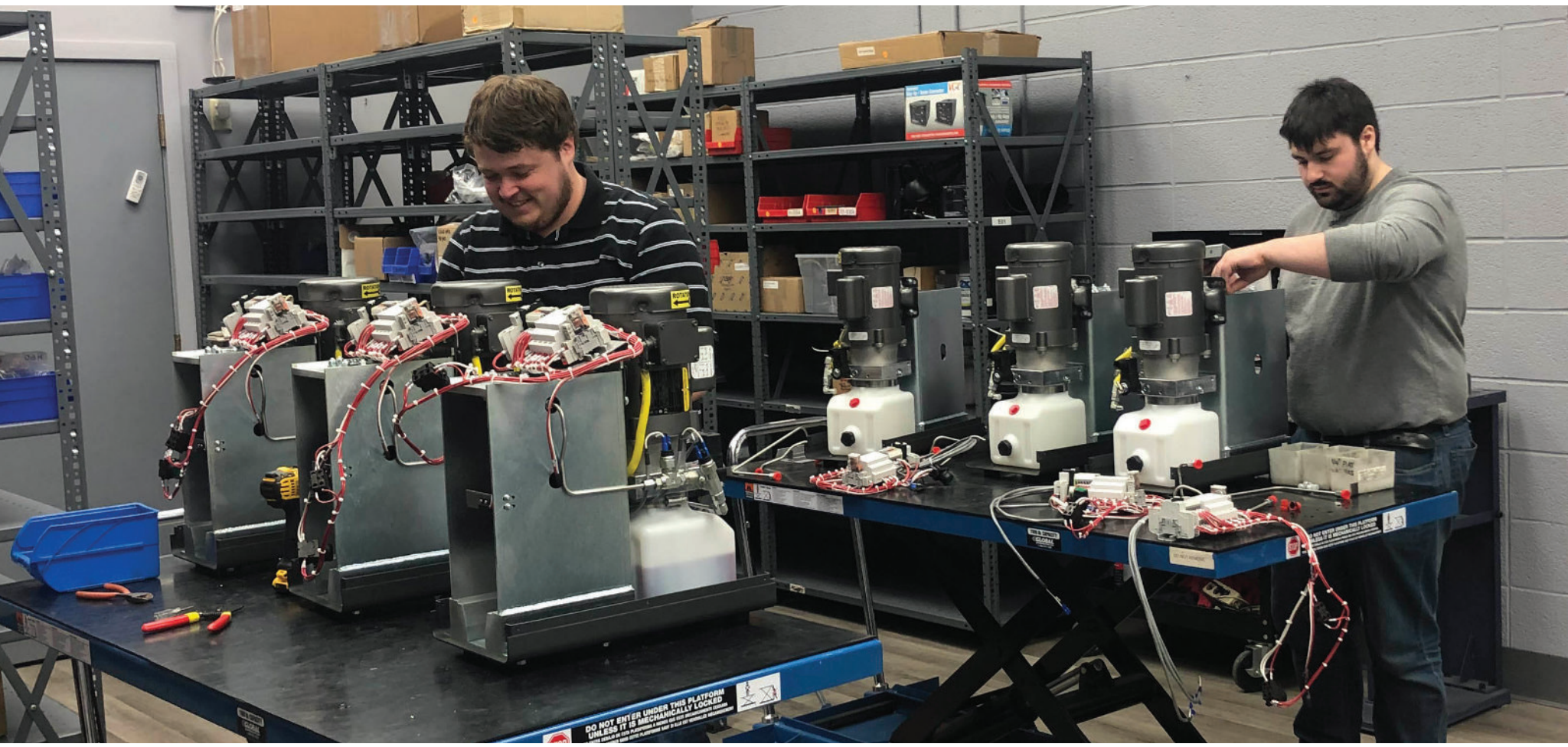
Shown is a hard drive shredded in an SEM 0305 hard drive shredder. Shredders are capable of shredding rotational hard drives and solid state drives, and are available as combo machines to destroy both HDDs and SSDs in one device.

DISINTEGRATE

Pictured is a solid state drive disintegrated in an SEM SSD2-HS high security solid state disintegrator. The final particle size is 2mm, the NSA mandate for classified solid state media.

WHO WE ARE

IN BUSINESS FOR OVER 50 YEARS, SEM'S SOLE PRODUCT LINE IS HIGH SECURITY INFORMATION DESTRUCTION EQUIPMENT AND OUR TARGETED AREA OF EXPERTISE IS INFORMATION END-OF-LIFE SECURITY.



Established in 1967, SEM is proud to be a US manufacturer that provides comprehensive end-of-life solutions for the protection of sensitive information in government and commercial markets. SEM data destruction devices are the premier high security choice available on the market today.

Whether paper, hard disk or solid state drives, tape, microchips, or any other type of media-bearing device, SEM has a solution that can sanitize classified and top secret information as well as controlled unclassified information (CUI), personally identifiable information (PII), personal health information (PHI), or any other type of sensitive data. SEM also produces customized equipment for size reduction solutions and for destroying off-spec or returned product for the medical device, gaming, security printing, and food industries as well as bank note/currency destruction for the US Federal Reserve and Central Banks throughout the world.

CONTACT US

5 Walkup Drive | Westborough, MA 01581

Phone: 508-366-1488
e-mail: contact@semshred.com

www.semshred.com

SEM®
Classified and High Security Data Destruction