

HIDDEN DATA STORAGE DEVICES: THE SECURITY RISK YOU CAN'T SEE

One overlooked data-bearing device can put your organization at risk.

IT asset disposition projects often begin with assumptions. Yet servers, desktops, firewalls, printers, and copiers can contain hidden storage devices that are easily overlooked and can expose your organization to serious risk.



**EXPOSURE OF
CONFIDENTIAL DATA**



**REGULATORY AND
COMPLIANCE ISSUES**



**AUDIT FINDINGS AND
INVESTIGATIONS**



LEGAL LIABILITY



**LOSS OF CUSTOMER
CONFIDENCE**

HIDDEN DATA IS MORE COMMON THAN YOU THINK

Data-bearing devices and non-volatile storage can be found in equipment throughout your organization, including:

RACK SERVERS



- Multiple HDDs and SSDs
- RAID controller cache
- NVMe M.2 drives
- Embedded flash
- PCIe expansion slots
- Motherboard storage

DESKTOPS & WORKSTATION



- Primary drive bays
- Expansion slots
- M.2 SSD
- Embedded flash
- Motherboard-mounted storage

FIREWALLS & NETWORK APPLIANCES



- Embedded flash
- SSDs
- CompactFlash
- SD cards
- Configuration storage

COPIERS & PRINTERS (MFPs)



- HDDs and SSDs
- Embedded flash memory
- Document and print history
- User credentials

NETWORK PRINTERS



- HDDs and SSDs
- Embedded flash
- Print queues
- Stored jobs
- Remaining paper jams



**THE CHALLENGE ISN'T DESTROYING DATA.
IT'S FINDING EVERY PLACE IT EXISTS.**

A secure IT asset disposition program should include multiple verification steps designed to identify hidden data-bearing devices before equipment is reused, recycled, or destroyed.

INSIST ON A **TRIPLE VERIFICATION PROCESS**

A strong data destruction program should never rely on a single inspection, a customer declaration, or one technician's assumption.



The goal is independent verification at multiple points, not confidence based on a single assumption.



ASSET-LEVEL ASSESSMENT

Identify which equipment is expected to contain data-bearing devices and document those expectations before processing begins.



PHYSICAL EQUIPMENT INSPECTION

Physically inspect every asset for internal, secondary, embedded, or overlooked storage devices regardless of what was previously reported.



TECHNOLOGY-BASED VALIDATION

Use software validation and serial-level documentation to reconcile discovered devices, document exceptions, and support final destruction records.

REAL-WORLD SITUATIONS

FINANCIAL SERVICES

WHAT THE CLIENT BELIEVED

Eight server cabinets had already been stripped of every drive before shipment.

WHAT WAS FOUND

During physical inspection, technicians discovered **86 overlooked drives** consisting of:

72 SSDs | **14** HDDs

Every drive was documented using DriveSnap AI™, securely destroyed, validated through Blancco, and included in the final reconciliation report.

WHY IT MATTERS

A single verification step would not have been enough. Multiple checkpoints turned a potentially serious security issue into a controlled exception that was documented, reconciled, and resolved.

TELECOMMUNICATIONS

WHAT THE CLIENT BELIEVED

A telecommunications provider shipped **300 servers** after confirming all drives had been removed.

WHAT WAS FOUND

Technicians discovered **30 remaining drives** containing sensitive operational data.

Each drive was removed, documented using DriveSnap AI™, securely destroyed, validated through Blancco, and included in the final reconciliation report.

WHY IT MATTERS

Verification protected the organization from relying on an upstream assumption that proved to be incorrect.

THE LESSON IS SIMPLE:

- ✓ Both organizations believed every drive had already been removed.
- ✓ Both projects still contained hidden data-bearing devices.
- ✓ Both situations were successfully resolved because the process included multiple independent verification steps.
- ✓ A mature IT asset disposition program verifies, reconciles, and documents.

Speak with a Data Destruction Specialist



(800) 731-1909



securis.com