IAITAM ACE 2025

ITAM - Another Brick In The Wall

Zero Trust in IT Asset Disposal: Strengthening Data Security & Compliance

By: Sunil Chandna, CEO BitRaser

BitRaser®

About Sunil Chandna

- CEO of **BitRaser**, a leading data erasure, diagnostics & verification software company by Stellar.
- **Co-founder, Stellar** (est. 1993) renowned for data recovery, file repair & email tools, with a strong presence in the USA and Europe.
- **Keynote Speaker** at international trade events on data destruction
- **Member of:**
  - Data Sanitization Experts group of SERI/R2
  - IEEE Security in Storage Working Group

ZERO TRUST – The Genesis

- **Origins In Cybersecurity**
  Zero Trust was coined in 2011 by cybersecurity expert and thought leader John Kindervag.

- **The Shift**
  The Zero Trust model moves away from the traditional perimeter-based security approach, which relies on firewalls and other technologies, towards a borderless enterprise environment founded on the principle of least privilege.

The Core of ZERO TRUST

Zero Trust is a security framework that assumes no entity—whether internal or external—should be trusted by default. Instead, continuous verification is required at every stage, including IT Asset Disposition.

NEVER TRUST, ALWAYS VERIFY applies to every asset.

- Requires **Strict Access Controls**
- Enforcement of **Least Privileged Access**
- Applies to **Data, Devices, and Users in the IT Asset Lifecycle.**

What is Least Privilege Access?

The principle of least privilege (PoLP) is an information security concept which maintains that a user or an entity should only have access to the specific data, resources and applications needed to complete a required task.

Why Zero Trust Matters in IT Asset Disposal?

Data breaches stemming from Improper IT asset disposal are a growing concern. With costs averaging millions of dollars per breach, organizations cannot afford to overlook ITAD security.

Zero Trust framework is a proactive approach to eliminate these risks.

Some Alarming Stats:

- Over **20% of all data breaches** are linked to lost or **improperly disposed devices**. [1]
- The human element was a component in **68% of breaches excluding malicious actors**. [2]
- As per IBM, the average **cost of a data breach in 2023 was $4.45 million**

1 [2023 Verizon Data Breach Investigations Report] ; 2 [2024 Verizon Data Breach Report]

Core Pillars of Zero Trust in IT Asset Disposal

1. **Define Media Disposal Policy & Roles**
   A Media Disposal Policy should lay disposal methods, compliance standards, roles, audit procedures, and secure data erasure guidelines.

2. **Identity & Access Management (IAM)**
   Enforce multi-factor authentication (MFA) and role-based access controls at every disposal stage.

3. **Data Encryption & Sanitization**
   Use advanced cryptographic techniques and certified data wiping tools to ensure data is irrecoverable.

4. **Continuous Monitoring**
   Implement end-to-end monitoring of the disposal process, chain of custody documents with real-time alerts.

5. **Maintain Certificate of Destruction (CoD)**
   Immutable CoD for audit purpose should be logged and maintained for anytime anywhere access.

6. **Vendor & Partner Assurance**
   Integrate third-party service providers into the zero trust framework. Align ITAD with industry standards (ISO 27001, NIST, R2v3, e-Stewards).

The Benefits of ZERO TRUST in IT Asset Disposal

1 **Mitigates Data Breach Risks**

Enforces strict, continuous validation even during disposal. Prevents lateral movement & maintains a secure chain of custody.

2 **Reduces Insider Threats**

Zero Trust minimizes Insider threats since no one is trusted implicitly.

3 **Enhances ITAD Transparency**

Zero trust practices extend into every stage of asset disposal, reducing vulnerabilities during hand-offs.

4 **Ensures Compliance**

Zero Trust helps meet rigorous requirements laid by law & regulatory frameworks.

5 **Builds Customer & Stakeholder Trust**

Demonstrates commitment to data security resulting in enhanced trust.

The Risks of Ignoring Zero Trust in IT Asset Disposal

Compromised Chain of Custody

Without robust monitoring, it's impossible to ensure assets are handled securely from end to end, leading to potential data leaks.

Weak Endpoint Protection for Remote Work

Without stringent endpoint security, lost devices can become gateways for cybercriminals to infiltrate company networks.

Theft & Loss of IT Assets

Without robust monitoring, it's impossible to ensure assets are handled securely from end to end, leading to potential loss of IT assets & compromise of business critical information.

Failure to Identify Anomalies

Zero Trust ensures continuous monitoring, and without it, unusual activities or unauthorized access attempts during disposal might go unnoticed.

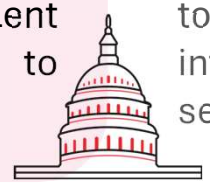
Absence of Zero Trust Security Model : Causes Data Breach

Morgan Stanley Data Breach:

Morgan Stanley faced a $60 million fine after failing to ensure proper data erasure during IT asset disposal. The bank's ITAD vendor resold decommissioned servers containing customer data, leading to a security breach. This incident highlights the risks of poor ITAD oversight and underscores the need for a Zero Trust approach to data destruction.

Recent Data Breach Case:

In Feb 2025, an ITAD employee based out of Washington, DC admitted to stealing & reselling hundreds of government devices, including laptops, tablets, & phones, from federal agencies & contractors. He misused his access during ITAD jobs to divert assets meant for destruction, issuing fraudulent Certificate of Destruction to cover up the operation.



FBI Data Breach Case:

In May 2024, An audit by the Department of Justice's Office of the Inspector General (OIG) has revealed significant lapses in the FBI's decommissioned electronic storage media containing sensitive information in data sanitization, inadequate tracking, and weak oversight that could led to potential exposure of classified information, posing significant security risks.

Integration of Zero Trust into IT Asset Disposal

01 Define Data Destruction Policy

Clear and Concise Policy that mentions:

- ✓ Scope & applicability
- ✓ Relevant compliance standards
- ✓ Data destruction methods
  - Onsite & offsite data sanitization procedure
  - Remote erasure for distant workforce
  - Documenting certificate of destruction (COD)
  - Regular auditing for process verification
- ✓ Roles of personnel (trained on data destruction)
- ✓ Retention & disposal timelines
- ✓ Reconcile devices decommissioned with CoD

02 Implement Least Privileged Access Policy

- ✓ Employees should only access what is necessary
- ✓ Authentication is required at every step
- ✓ Revoke access once the task is complete

03 Classify Data and Asset Inventory

Categorize IT assets based on:

- ✓ Device type: laptops, desktops, servers, mobile
- ✓ Storage technology: HDDs, SSDs, hybrid drives
- ✓ Data sensitivity: confidential, public, internal

Integration of Zero Trust into IT Asset Disposal

04 Implement On-Premise Data Destruction

- ✓ Basis data destruction policy, choose the right data destruction method
- ✓ Set up dedicated data erasure station within company premises or hire a certified service provider for performing on-premise wiping
- ✓ Hire a skilled team of technicians
- ✓ Maintain audit trails
- ✓ Perform data destruction verification

05 Implement Off-Site Data Destruction

- ✓ Select a certified ITAD vendor with R2, e-Stewards, or ADISA certifications
- ✓ Erase data before devices leave company premises, even if destined for shredding.
- ✓ Maintain chain of custody documentation for secure asset transportation with real-time tracking to prevent data or device theft in transit.
- ✓ Seek detailed audit reports from ITAD vendors.

Integration of Zero Trust into IT Asset Disposal

06 Implement Remote Data Sanitization

- ✓ Enforce erasure policies for employee offboarding
- ✓ Automate erasure when an employee leaves or a project ends.
- ✓ Deploy remote erasure software to securely wipe data from remote endpoints used by WFH employees
- ✓ Automate erasure via centralized enterprise management system initiate erasure remotely
- ✓ Obtain proof of erasure automatically

07 Define Criteria to Select Right ITAD Vendors

- ✓ Must have either, R2, e-Stewards, ADISA ICT, NAID AAA certification.
- ✓ Real-time tracking of assets in transit
- ✓ Adherence to industry standards for data destruction
- ✓ Reconcile the picked devices with received assets and processed items.
- ✓ Ensure capability to apply advanced data erasure techniques (e.g., Block Erase / CE)

- Zero Trust in ITAD eliminates implicit trust and enforces verification.
- Implement a clear, documented ITAD policy with strict oversight.
- Use certified data erasure tools to prevent data recovery.
- Regularly audit ITAD processes and ensure compliance with industry standards.
- Secure remote data erasure is essential for hybrid and remote workforces.

BitRaser

Scan to Read
Full Article

Connect With Me!

sunil@stellarinfo.com

+1 844-775-0101

https://www.linkedin.com/in/sunilchandna/