Sponsored content | White paper

IT asset disposition is broken—and it's costing you

A call to reimagine ITAD as a strategic focus, not an operational checklist item

CIO

Sponsored by IRON MOUNTAIN® ASSET LIFECYCLE MANAGEMENT

Organizations routinely manage all sorts of hardware across data centers, end-user environments, and global operations, which means they must be able to securely retire those assets when the time comes. Yet, while critical to reducing risk and maintaining compliance, IT asset disposition (ITAD) remains an afterthought for many businesses.

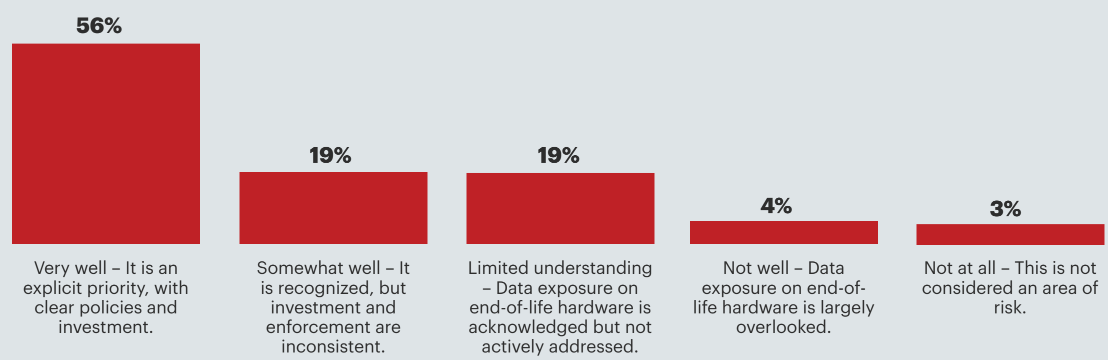
Despite growing awareness of the data risks involved, IT practitioners still think of ITAD as a logistical end-of-life task rather than a core security function. As a result, their approaches are fragmented, underfunded, and inconsistent — leaving gaps that present significant risks.

This white paper shares new research findings that illustrate this disconnect and makes the case for elevating ITAD to a strategic imperative that reduces risk, drives operational improvements, and brings financial benefits.

Awareness is high, but execution falls short

Most IT decision-makers understand that end-of-life devices present data security and compliance risks. In a recent Foundry MarketPulse survey, 56% identified end-of-life data exposure as a top concern, with 64% providing regular ITAD-related training.

Leadership understanding of the risks associated with data exposure on retired, or end-of-life IT hardware



In practice, however, few have standardized processes, clear ownership, or sufficient budget. One of the main reasons is that ITAD is often miscategorized — assigned to facilities or procurement instead of risk or security teams — and treated as a physical asset concern rather than a data lifecycle priority.

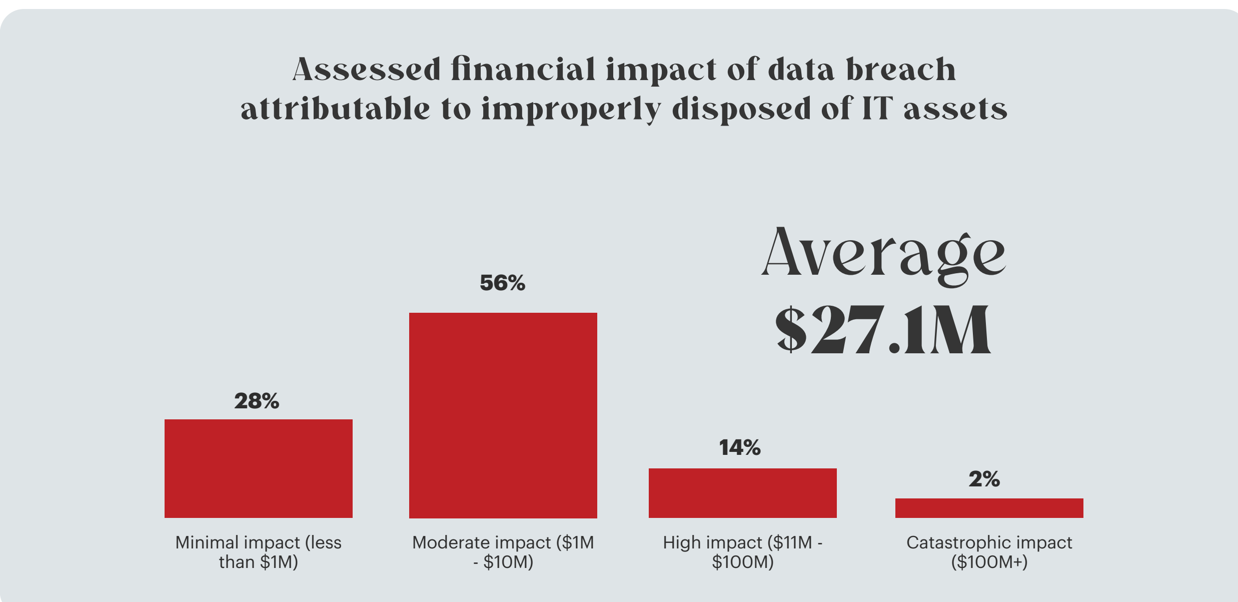
This mindset, reinforced by outdated habits and lack of internal alignment, leads to inconsistent execution and underfunding. Further, while decision-makers focus resources on active threats, such as malware and intrusions, they overlook the latent risks associated with improperly handled devices. Additionally, because ITAD often happens at the end of a device's life, it tends not to receive the same level of investment as live infrastructure. The average company allocates just 5% of its security budget to ITAD and nearly two-thirds of organizations spend less than that, the survey found.

The end result: Despite its role in protecting sensitive data and ensuring compliance, ITAD remains an under-prioritized part of enterprise IT operations, with most organizations failing to treat it as a core business priority and leaving behind unrealized financial benefits that could offset costs related to improved practices.

To close this gap between risk and resourcing, organizations need to formalize ITAD programs as part of their broader compliance and security strategies. That includes assigning ownership, aligning budgets, and standardizing policies across business units and geographies. It also requires involving a broader set of stakeholders. ITAD touches multiple functions — including IT, security, procurement, finance, and sustainability — all of which have a vested interest in reducing risk, managing costs, and supporting ESG goals. When these teams coordinate through a centralized program, they can improve data protection, reduce unnecessary spending, and recover residual value from retired assets.

The risks of inadequate ITAD

Improper ITAD exposes companies to significant risk, including data breaches, loss of customer trust, regulatory scrutiny, financial penalties, and lasting brand damage. Survey respondents estimated the cost of a breach tied to improper ITAD to be $27.1 million, on average.



To further illustrate the risks, consider this real-world example: A large global bank hired a third-party vendor to retire IT devices that contained personally identifiable information. The vendor neither properly sanitized the devices nor provided certificates of destruction for all assets, and the devices were later resold online. The bank was found in violation of data protection regulations and held responsible for the vendor's mishandling. The breach made worldwide headlines, which hurt the firm's reputation, and resulted in tens of millions of dollars in federal fines.

The poor chain of custody and lack of certification that led to this incident are common ITAD vulnerabilities. Other weak points include:

- Inconsistent ITAD policy enforcement and management of multiple vendors across distributed environments
- Reliance on third parties without appropriate credentials
- Gaps in documentation and audit trails
- Data sanitization methods that do not meet industry standards (e.g., NIST 800-88)

Organizations should view ITAD as a core component of their data security posture, especially as scrutiny grows around global data protection and compliance with regulations such as HIPAA and GDPR. Despite these vulnerabilities and regular high-profile incidents, however, many companies still underestimate their risk level. Fifty-six percent of survey respondents said their risk of exposure due to gaps in ITAD efforts is low, while only 44% admitted to at least moderate risk exposure — suggesting overconfidence, inconsistent standards, or both.

A fragmented approach increases risk

The emergence of distributed organizations, remote workforces, and new work styles has created new challenges. End users today may be based in various locations, travel frequently, and have multiple devices, all of which complicates hardware asset management.

In these scenarios, many organizations take multiple ITAD approaches and even rely on multiple vendors across different regions and business units, often in the name of convenience and cost-effectiveness. But this strategy can result in inconsistent enforcement, miscommunication, and poor visibility.

Without centralized control, it’s difficult to ensure teams are following policy and securely destroying data. It also complicates audit readiness; 24% of survey respondents said their organization would require at least one month to prepare for an audit.

By unifying ITAD processes across regions and units and standardizing on one provider, businesses can help ensure consistent global compliance, reduce vendor-related risks, and improve their reporting and chain-of-custody control. To do so, they need to formally designate ITAD as part of their broader security and compliance strategies, acknowledge it as a core data management function, and create programs complete with dedicated policies, oversight, and accountability.

Ownership of these programs typically falls to IT, but they require coordination and regular communication with other key stakeholders, including ESG, procurement, security, and finance teams. Eliminating the silos that exist among these departments strengthens governance, improves alignment, and enables more informed decision-making about end-of-life asset management.

The business case for ITAD

When properly implemented, ITAD's benefits extend beyond risk reduction. It can generate tangible value across multiple areas of a business.

For example, secure ITAD processes minimize e-waste and reduce carbon emissions by encouraging device refurbishment and reuse as higher-value alternatives to e-waste recycling, contributing more to ESG goals. Many devices still hold financial value at end of use, some of which organizations can recover through resale or donation after proper data sanitization. This lowers total cost of ownership, at times significantly offsetting ITAD vendor costs, while enhancing corporate responsibility and social impact initiatives. Additionally, centralized ITAD strategies reduce internal complexity, which improves efficiency.

Despite these benefits, organizations may struggle to quantify and communicate the full value of their ITAD programs. They would do well to consider key performance indicators including:

- Prevention of data breach and regulatory noncompliance fines
- Reduced IT procurement costs due to improved device retrieval and redeployment rates
- Avoidance of penalty fees for late lease returns
- Landfill avoidance and carbon emission reduction, comparing reuse to recycling
- Vendor reduction and other efficiency gains from consolidated management

Monitoring such metrics will help build a compelling business case for ITAD and demonstrate how it supports other business goals. In turn, that combats the misconception that ITAD is a logistical task, not a strategic initiative like other security and compliance efforts.

An argument reframing ITAD in such terms should resonate with the concerns of multiple teams, including:

- **Risk and security teams:** secure data destruction and breach prevention
- **Finance and procurement:** return on investment (ROI) and cost optimization
- **IT:** centralized oversight and reduced asset management friction
- **ESG:** measurable environmental impacts

Supporting these arguments with accurate, updated data is critical for transforming ITAD into a strategic business function.

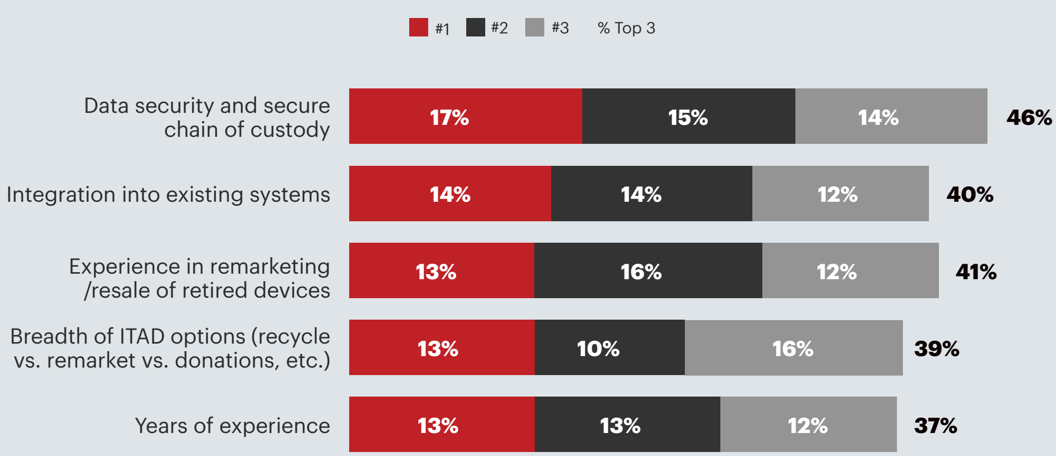
Top drivers of ITAD investment

Although the business case for ITAD is broad, security remains the top investment driver. A high-profile breach is the top motivator for IT asset lifecycle management, with 26% of respondents identifying it as a trigger. Financial and regulatory reasons are almost equally influential, however, with 20% identifying increased regulatory pressure, clear financial ROI, and demonstrated compliance benefits as drivers.

Factors that would most increase ITAD investment

Security is also the main factor in ITAD vendor selection. When asked to name their three most important criteria, 46% of respondents included data security and secure chain of custody capabilities.

Top 3 most important drivers in selecting an ITAD vendor



The path forward

For organizations looking to elevate the role of ITAD, the path forward starts with formalization. This means explicitly prioritizing ITAD as a core component of overall data security and compliance strategies, moving beyond ad hoc processes and assigning clear ownership so it receives the attention and policy support it requires.

The next step is to unify ITAD oversight across regions, departments, and asset types, which allows for consistent policy enforcement, improved visibility, and streamlined internal coordination. Standardized processes and documentation enable teams to respond more quickly and confidently to audits while reducing the risk of gaps in data destruction or compliance tracking. Organizations should also ensure regular collaboration between ITAD owners and adjacent functions such as compliance, finance, procurement, and ESG. These cross-functional conversations are essential for aligning goals, identifying overlapping priorities, and maximizing value.

Vendor selection is equally important. Organizations that work with multiple ITAD providers inevitably discover that each has varying standards, certifications, and capabilities, resulting in a fragmented approach that increases complexity and undermines consistency. By consolidating ITAD with a single, certified partner that offers secure chain of custody, centralized program management, and robust reporting, organizations can better safeguard data, simplify operations, and generate clearer performance insights. The right partner should also support broader sustainability goals through environmentally responsible IT reuse and e-waste recycling and provide detailed reporting that quantifies outcomes such as emissions reduction, landfill diversion, and value recovery.

With these elements in place, ITAD can evolve into a fully integrated function that protects data, supports ESG priorities, and contributes to stronger business performance.

This custom research study was commissioned by Iron Mountain Asset Lifecycle Management. To learn how Iron Mountain can help your organization mitigate risk and turn ITAD into a strategic advantage, visit www.ironmountain.com/ALM.