Market Pulse

Sustainable, Secure ITAD Is a Must for Business Leaders

The current global business disruption is changing technology needs overnight. But new IDG research reveals that many organizations are still working to bring their IT asset disposition (ITAD) program in line with the demands of today's IT lifecycle management. Organizations are struggling with ITAD strategy, and many are not following best practices.

In these uncertain times, where every dollar is scrutinized and IT budgets are under the microscope, it is more important than ever for organizations to ensure their ITAD program provides value in line with business objectives. At the same time, they must ensure that ITAD is carried out in a secure and sustainable way.

To determine the connection between IT asset disposition and corporate sustainability goals, IDG surveyed IT leaders in the US and UK working in financial services, technology, or healthcare and life sciences at organizations with 5,000+ employees. The goal was also to understand where organizations stand with current ITAD practices, their objectives for these programs, and the challenges that they face.

With more pressure than ever to comply with data security and privacy regulations, organizations need an ITAD strategy that offers secure disposition practices. Organizations now also place a premium on environmental priorities when it comes to ITAD.

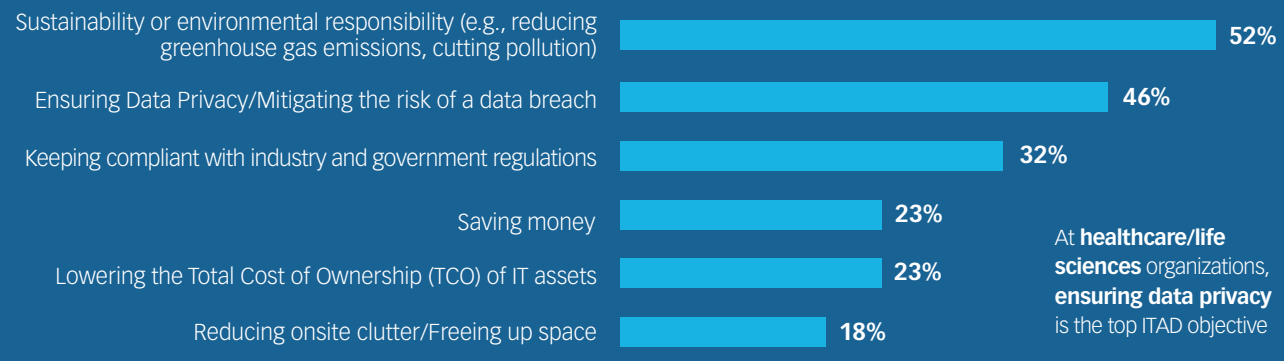
Sustainability: The New Driver for ITAD

Organizations want—and need—to be more environmentally sustainable. Being known as a sustainable company is now a point of pride and corporate responsibility. In fact, Executive management may appoint "green" C-level IT officials to keep an eye on environmental programs.

This move toward greener business practices is driven in part by customers preferring to work with organizations that are mindful of environmental sustainability, But it's also driven by the shifting priorities of investors, who may want to put their dollars into more environmentally conscious organizations and those with a lower carbon footprint.

As a result, IT leaders are now tasked with implementing sound environmental practices in both the investment

Figure 1. Primary ITAD Objectives



At **healthcare/life sciences** organizations, **ensuring data privacy** is the top ITAD objective

Source: IDG

CIO FROM IDG

IRON MOUNTAIN®

and the disposal of IT assets for their organizations. Top-level management wants to ensure that when disposing of IT assets, the organization is doing everything it can to stand up programs that reflect their overall sustainability strategy.

> *The message is clear: sustainability is now a key corporate objective and ITAD is an integral part of delivering on that mission.*

This attitude is reflected in the IDG survey, which revealed that 71% of organizations see ITAD strategy and decision making as central to their sustainability or environmental responsibility strategy.

> *According to 52% of survey respondents, the top objective for ITAD programs is to meet sustainability goals.*

Other top objectives include protecting data privacy (46%) and ensuring compliance (32%).

The data further illuminates that sustainability is a top driver in ITAD, as e-waste levels are at an all-time high. According to a recent report by the World Economic Forum, 50 million tons of e-waste are produced globally each year. If left unchecked, that number could more than double to 120 million tons by 2050.

Responsible technology use and disposal is essential to any organization's environmental and sustainability program—and those programs are also growing in importance, according to CIO.com. More CIOs are putting programs in place to limit their organization's carbon footprint and set an example with sustainable technology practices.
While compliance was named as the primary driver of sustainability goals (54%) in the IDG survey, 52% of all respondents report that core values are also a top objective. The message is clear: sustainability is now a key corporate objective and ITAD is an integral part of delivering on that mission.

The Heat Is on ITAD – but Poor Practices Remain

While a desire to move environmental initiatives forward with ITAD is a core goal for organizations, the research also finds, unsurprisingly, that security and data privacy are integral factors in any solid ITAD strategy. Data security (48%) tops the list of concerns regarding the management of obsolete and retired IT devices, followed by the ability to meet local, state, federal, and industry regulatory requirements (36%).

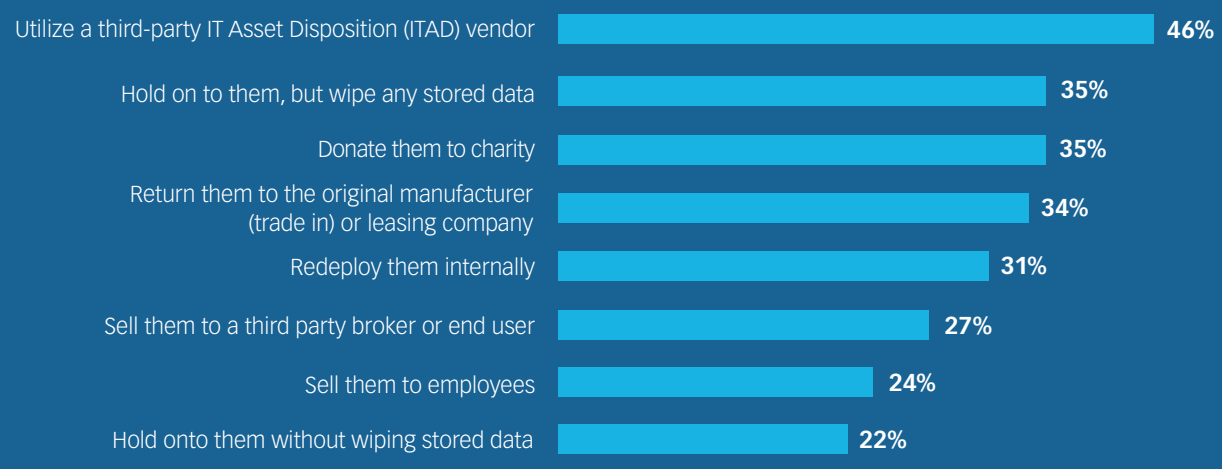
One factor influencing these concerns is an increasingly demanding compliance and regulatory landscape. Regulatory demands mean it is critical that organizations ensure that all data has been removed securely from IT assets. The General Data Protection Regulation (GDPR), and the new California Consumer Privacy Act (CCPA), for example, both regulate how organizations handle the data of certain citizens.

Organizations that do not comply with rules for how that data is managed, stored, and disposed of face significant fines and penalties.

But despite the widespread recognition that a solid ITAD program is essential for data security and regulatory compliance, many organizations are still ignoring ITAD best practices.

Half the respondents said their organization is holding on to at least some end-of-life IT assets. Other poor ITAD practices named include not wiping stored data on assets retained (22%) and either simply throwing retired assets away, or stockpiling them in-house, unused (37%).
The implications for failing to securely destroy,

Figure 2. Current Methods of Handling End-of-Life IT Assets



Source: IDG

recycle, or remarket end-of-life electronics responsibly are serious. In addition to regulatory penalties, damage to brand reputation and data breaches are very real and potentially expensive. The Ponemon Institute's 2019 annual Cost of a Breach survey reports that the average total cost of a data breach is $3.92 million.

The results of a recent research report from The Ponemon Institute also indicate that customers demand security: 65% of respondents said a data breach had caused them to lose trust in the organization, and 27% noted they would discontinue their relationship with that organization after a breach. IT leaders also understand the damage a breach can cause as 55% of IT professionals believe that a data breach would negatively impact reputation, according to Ponemon.

Protecting proprietary and sensitive information is a cornerstone of any responsible ITAD program. But any expectation of safe data handling is forfeited if retired IT assets are not given the same care and handling as active equipment. Failing to wipe retired assets before disposing of them, or allowing them to sit in-house without proper security, can put organizations at high risk for a data breach, which can lead to loss of trade secrets and other private corporate information.

IT Leaders Have an Opportunity with ITAD

Within organizations, management of IT asset disposition falls to two main groups: IT and IT security. But the survey found that the CIO or head of IT most often has primary responsibility for ITAD. Because of this, IT leaders, particularly CIOs, have an opportunity to help steward both corporate responsibility and best-in-class security and privacy practices.

To that point, the survey found three key areas where IT leadership can ramp up involvement in ITAD strategy (and support core organization values):

- **Centralizing IT asset management** – IT asset management is a precursor to the ITAD process. IT departments deploy, maintain, and keep track

of IT assets, and determine when they need optimization or replacement. Centralizing these efforts can also help organizations with the disposition process at the end of an asset's lifecycle to ensure the equipment is tracked properly, and handled appropriately and securely, when it is retired.

■ **Advocating for an increase in recycling** – As the data revealed, many organizations are allowing retired unused assets to simply sit in-house, which is neither secure nor environmentally sound. The CIO can champion a more consistent effort to ensure assets are wiped securely and recycled in line with green practices.

■ **Identifying assets that can be refurbished for reuse** – In line with the desire to be seen as environmental stewards, the CIO has an opportunity to advocate for refurbishing of equipment whenever possible, which can offer both environmental benefits and cost savings for the organization.

The opportunity for CIOs to play an integral role in both brand protection and supporting corporate sustainability initiatives is apparent through ITAD. The CIO's role in sustainability will only grow as more organizations seek to implement environmentally sound practices, and ITAD is a critical component of those efforts. As the research finds, now is the time for CIOs to lead their organizations into an era of sustainable and secure ITAD practices.

Evaluating ITAD Vendors? Keep These Notes on Hand

Eight in ten respondents (80%) to the IDG survey say their organizations are likely to consider working with a third-party provider of managed asset deployment services over the next 12 months. If your organization fits that bill, keep these notes on hand.

- When evaluating ITAD vendors, data security is the top decision criteria (90% rating critical/very important).
- Also high on the list of criteria: brand trust (85%), secure chain of custody (83%), and environmental and social responsibility (82%).
- Transparency is rated as the most important capability in an outsourced ITAD partner (86% rate critical or very important).

For more information, visit
www.IronMountain.com/SITAD
(877) 654-3809

The Bottom Line

A secure and sustainable ITAD strategy is imperative for businesses today, as IT decision makers (ITDMs) are increasingly focused on sound environmental practices and want to safeguard sensitive data in the IT asset disposition process. In addition, the regulatory and compliance landscape is putting pressure on organizations to ensure data is handled properly and in line with global privacy rules. However, IDG research reveals that ITAD practices are still lacking in many organizations. ITDMs must ensure their ITAD program meets security and sustainability objectives and offers as much value as possible to the business.

Now is the time to update your ITAD program and work with a trusted partner that has defined procedures for handling end-of-life electronics in an environmentally-safe manner. visit **IronMountain.com**.

CIO FROM IDG

IRON MOUNTAIN®