blancco

2026 State of Data Sanitization Report

The hidden cost of end-of-life data security anxiety

Confidence in data sanitization is high—but the reality is more complicated.

Organizations report high levels of assurance in their data sanitization practices, yet their actions suggest a different story.

Based on responses from 1,460 IT, compliance, and sustainability leaders across regulated organizations worldwide, this report examines how organizations are managing data at the end of the asset lifecycle—and where gaps between data security confidence and operational reality remain.

Intro: Decommissioned tech—where confidence is tested

All organizations hold sensitive data—their own, and their customers. They recognize the value this data would have in the wrong hands. Yet while data is vigorously protected in active use, new vulnerabilities crop up when drives or devices storing that data need to be decommissioned for replacement or retirement.

At these stages, IT leaders face competing pressures. Not only do they need to protect sensitive data from getting into the wrong hands, but they must also meet regulatory requirements for data privacy and reporting, manage expectations around e-waste and environmental sustainability, and respond to the ways technology trends impact data volumes and business costs.

Organizations typically navigate these pressures through various forms of data sanitization, the process of making data unrecoverable from storage media. Done correctly, sanitization prevents previously stored data from being accessed from used devices. Depending on the method of sanitization, assets can often be redeployed for additional use.

The good news is, when it comes to removing data from decommissioned assets, many respondents are confident in their sanitization practices. But as organizations use AI to process, gather, and create more data, and as threats become more sophisticated, confidence alone is not enough.

The findings in this report suggest that while organizations believe their processes are effective, their behaviors—ranging from inconsistent sanitization practices to the continued destruction of functional hardware—indicate the presence of real underlying risk as well as uncertainty about whether data has truly been removed.

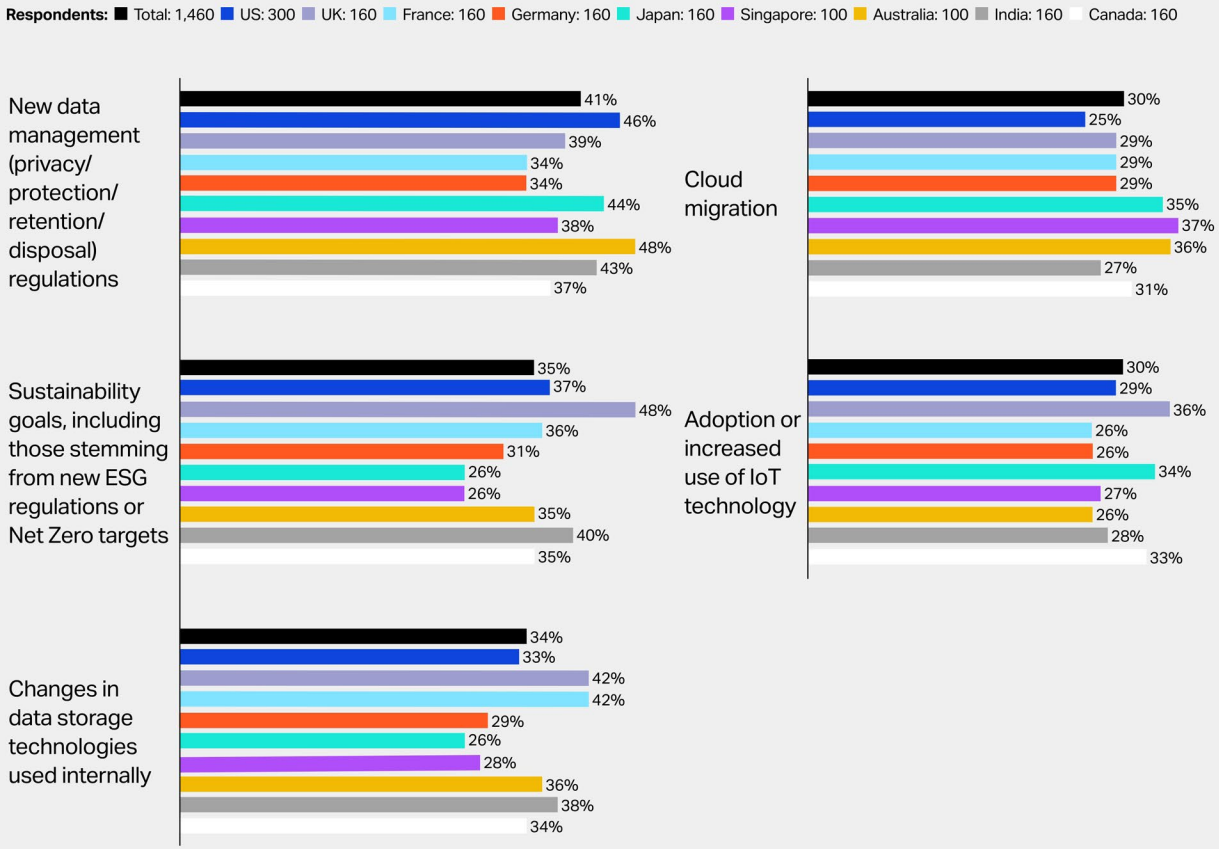
Key findings: Anxiety is driving uncertainty and waste

A number of data privacy and protection regulations require organizations to securely delete or render data inaccessible when it reaches end of life, or is no longer needed, regardless of where it lives.

Perhaps unsurprisingly then, 41% of respondents reported that data privacy and protection regulations were the number one driver behind end-of-life data management changes.

Beyond regulation, changes in data storage technologies, cloud migration, sustainability, and vendor risks are also influencing this stage of data management.

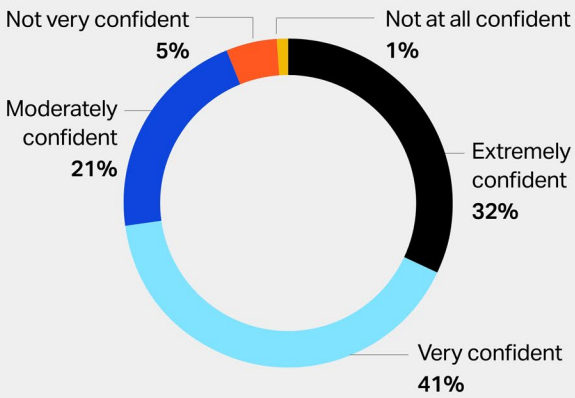
In 2025, which of the following organizational or industry developments most impacted end-of-life data management changes in your organization?



Key findings: Anxiety is driving uncertainty and waste continued

Even while adopting new data management processes, 94% of organizations reported being moderately, very, or extremely confident that their practices render drives and devices free of data before disposal.

How confident are you that data is fully sanitized before drive or device disposal?



There is, however, a conflicting story.

Organizations continue to use inconsistent data sanitization methods at the end of the device lifecycle. Many incorporate approaches that do not produce complete data removal or that do not verify that data has been destroyed. This means some of that confidence may be misplaced.

At the same time, data security anxiety is driving many organizations to physically destroy valuable, still-functional data storage devices—despite a desire to operate more sustainably and a need to manage **changing hardware costs**.

These behaviors point to a shared issue: uncertainty about whether data has truly been removed and rendered irrecoverable.

There's good reason for that uncertainty. Poor end-of-life data management can result in data leaks—an unintentional exposure of sensitive information through human error or misconfiguration.

More than a third (38%) of organizations report experiencing a data leak in the past year. While 46% cited improper network configurations, a significant number are linked to data storage assets changing hands.

Notably, 32% of the respondents who experienced a leak attributed it to redeployed drives or devices retaining sensitive data. This suggests that confidence in device decommissioning processes isn't always translating into effective data protection.

A stacked regulatory environment is driving complexity and cost

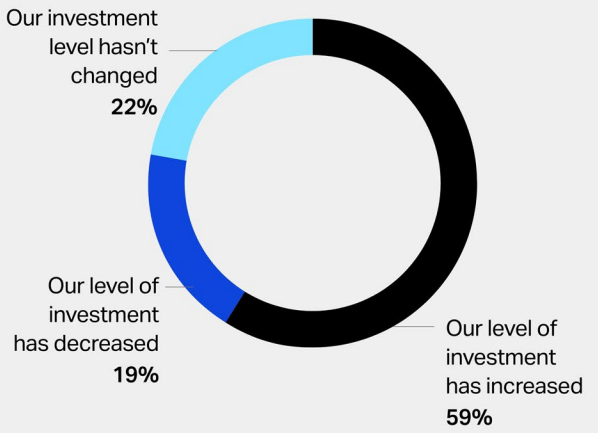
Organizations are still adapting to regulatory demands—and spending more to keep pace. Compared to the previous year, 2025 was not defined by a wave of newly introduced data privacy and protection laws. Instead, organizations are operating in a phase where previously passed regulations are coming into force—and must be implemented in practice.

New requirements related to artificial intelligence are also beginning to layer on top of existing data protection obligations, adding further complexity to an already demanding regulatory environment.

As a result, nearly 60% of organizations increased spending related to data privacy and protection compliance compared to the previous year. In some countries, including within the U.K. (74%), U.S. (70%), and Singapore (70%), the percentage is even higher.

On average, organizations reported spending 40% more than in 2024. This is consistent with last year's report, indicating year-on-year growth in investment.

How did your spending on data privacy and protection compliance change in 2025 compared to 2024?

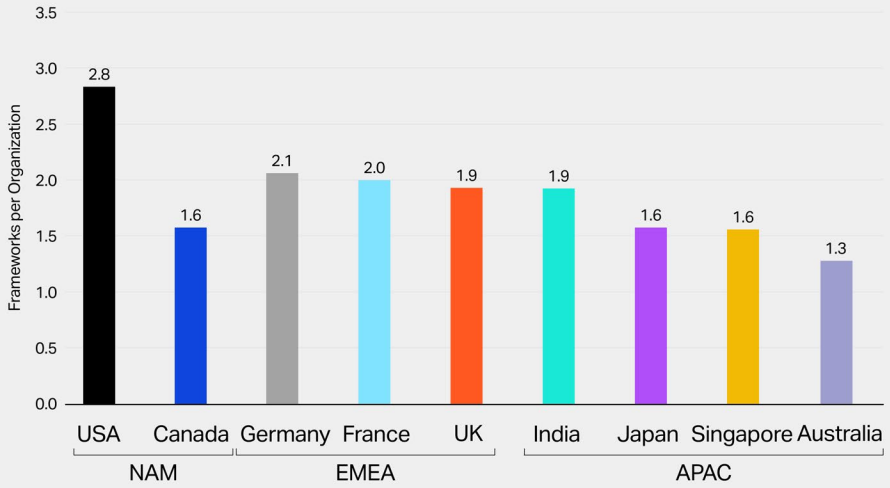


A stacked regulatory environment is driving complexity and cost

continued

Regulatory exposure is increasingly multi-layered. Based on a representative set of major data privacy and protection regulations included in this study, organizations are managing multiple overlapping obligations across jurisdictions and industries, rather than a single dominant requirement. This increases operational complexity and raises the stakes for consistent, auditable execution across the data lifecycle.

Average Number of Data Protection and Privacy Frameworks per Organization, by Country

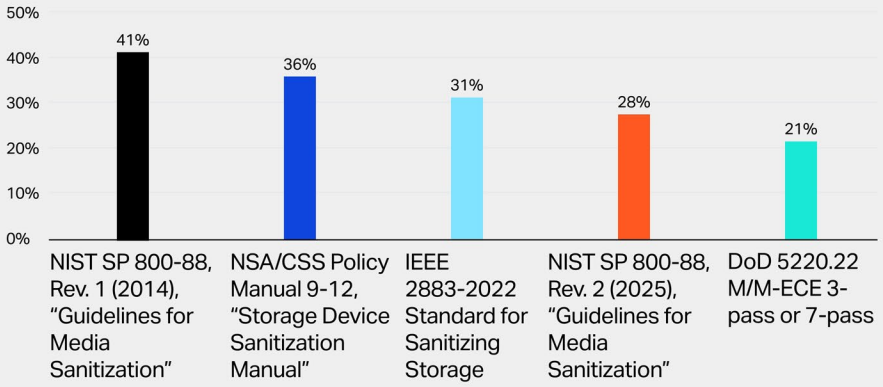


Based on reported compliance with selected major regulatory frameworks included in the survey.
USA: CCPA/CPRA, HIPAA, NYCRR Part 500, NY SHIELD, GLBA, FACTA, SOX, state-level regulations | **Canada:** PIPEDA, provincial privacy laws, CSA requirements | **Germany:** GDPR, BDSG, BSI Act, PDPA/PDSG, CSRD | **France:** GDPR, DPA (French Data Protection Act), CNIL, CSRD, HDS | **UK:** UK GDPR, EU GDPR, SECR | **India:** DPDP Act, IT Rules (SPDI), CERT-In | **Japan:** APPI, PPC-FSA, 2G3M | **Singapore:** PDPA, Cybersecurity Act | **Australia:** Privacy Act, ASIC

This is where industry data sanitization standards play a critical role. Standards such as NIST SP 800-88 and IEEE 2883 provide guidance on how to securely and irreversibly remove data from devices.

As technology changes, staying up to date enables organizations to make sure they're matching the most effective methods to data sensitivity and device types, tying their decommissioning confidence to accepted best practices.

Which of these technical standards does your organization regularly use within its asset-disposition or data-destruction processes?



While adoption of newer standards is increasing, legacy approaches remain common. Continued use of older frameworks and destruction-first methodologies suggests that organizations are balancing modern practices with familiar approaches.

Stolen, lost, and redeployed devices are causing data leaks

More than a third (38%) of organizations report experiencing a data leak in the past year.

While more organizations report malicious data breaches (58%), data leaks—unintentional exposures caused by human error or misconfiguration—remain a significant and persistent risk. Most leaks (46%) are attributed to improper network configurations. However, a substantial proportion are linked to data-bearing assets changing hands.

Notably, 32% of organizations that experienced a leak attribute it to redeployed drives or devices retaining sensitive data. This highlights a critical gap: data is not always fully removed before assets are reused.

Additional leaks are linked to lost (42%) and stolen (25%) devices, which may occur during everyday use or throughout the decommissioning process.

Regional differences are also evident. Redeployment-related leaks are more common in the U.S. (40%) and Australia (41%), and highest in Singapore (45%).

Many of these incidents are preventable. They point to weaknesses in how organizations manage data at the end of the asset lifecycle—particularly when assets leave controlled environments without verified data sanitization.

38%

of respondents report suffering a data leak in the last twelve months.

1 in 8

organizations reported a data leak due to redeployed devices or drives with sensitive data left behind.

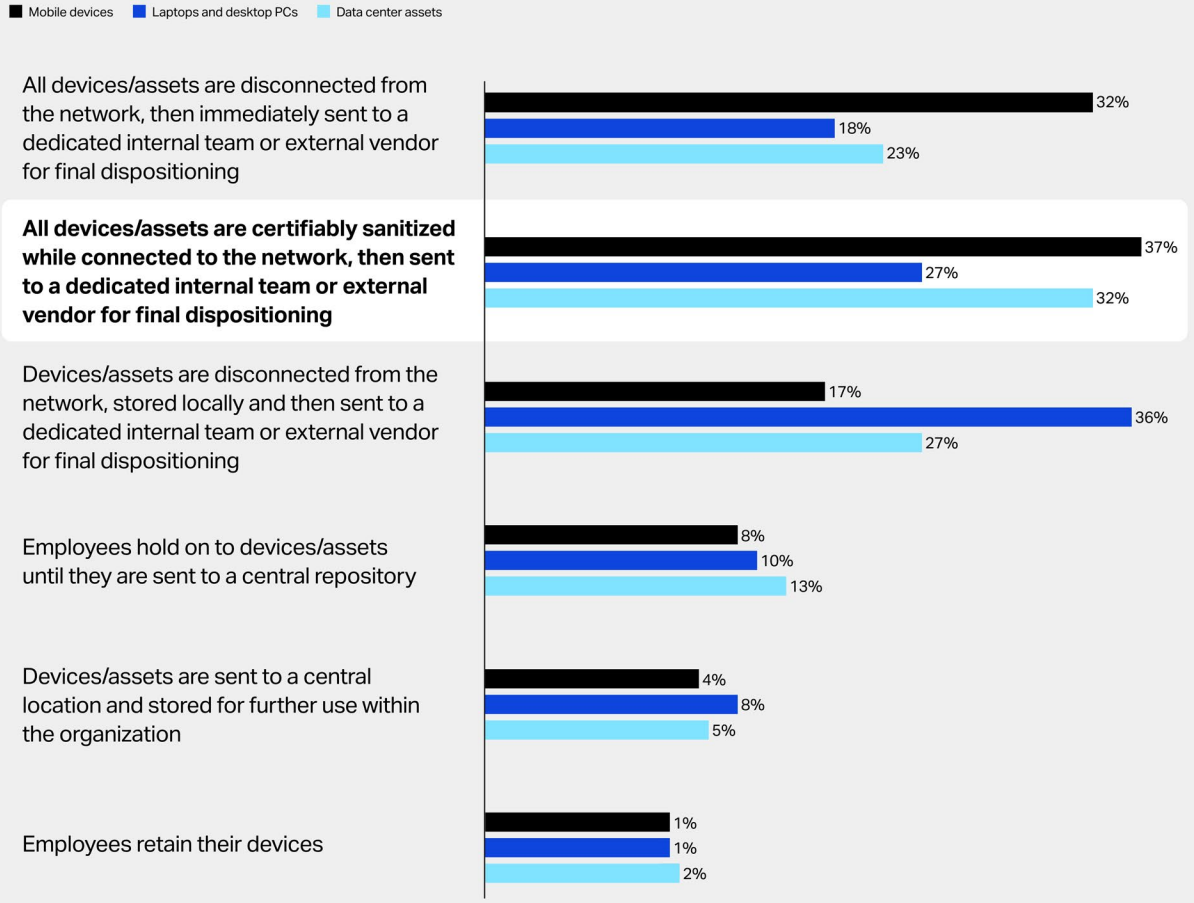
Best practice sanitization is not universal

The ideal, most secure scenario for decommissioned assets is to remove data as soon as possible, while devices are still connected to the network.

This ensures data is irreversibly removed and erasure is verified before assets are transported, stored, or redeployed.

However, averaging across all device types, less than a third of organizations have this practice in place.

How are endpoint devices and data center storage assets dispositioned at present?



Best practice sanitization is not universal continued

Other common approaches, such as devices being disconnected from the network, stored locally, and then sent for final dispositioning (36% for laptops and desktop PCs), introduce vulnerability gaps. During this time, data-bearing devices may be lost, stolen, or otherwise leave organizational control before data has been securely removed.

Cautionary Tales

Improper device disposal sometimes results in data leaks that make the headlines. In the Netherlands last year, drives bought at a flea market were found to contain sensitive medical data. In another case, a driver for an IT disposal company was found to have been stealing and selling equipment.

These cases show the risks of not sanitizing data as soon as possible – when removed from the network without sanitization, there will always be a risk of a data leak.

Data destruction can occur later in the process, but not all practices provide the security that regulated enterprises need.

Common data destruction methods that fall short of sanitization

Reformatting

Data can often be recovered using readily available forensics tools, yet this method is used by 33% of organizations for laptops and desktops. In the UK, France, and India, the percentage is slightly higher (36%).

Paid software-based overwriting tools without certification

This method is used by 22% of organizations for laptops and desktops and 19% for data center assets, but it may not align to an industry standard or verify the erasure has been successful.

Organizations often use multiple methods across different devices or scenarios. While this may reflect differences in device type or perceived sensitivity, it introduces inconsistency—making it more difficult to ensure that data is fully removed across the enterprise.

This inconsistency helps explain why data leaks persist, even as organizations report high levels of confidence in their data sanitization practices.

There's also an organizational component. While 89% of organizations report having asset sanitization policies in place, only 61% say those policies are implemented and communicated across the business.

This gap between policy and practice increases the likelihood that data is not handled uniformly as assets move through the lifecycle.

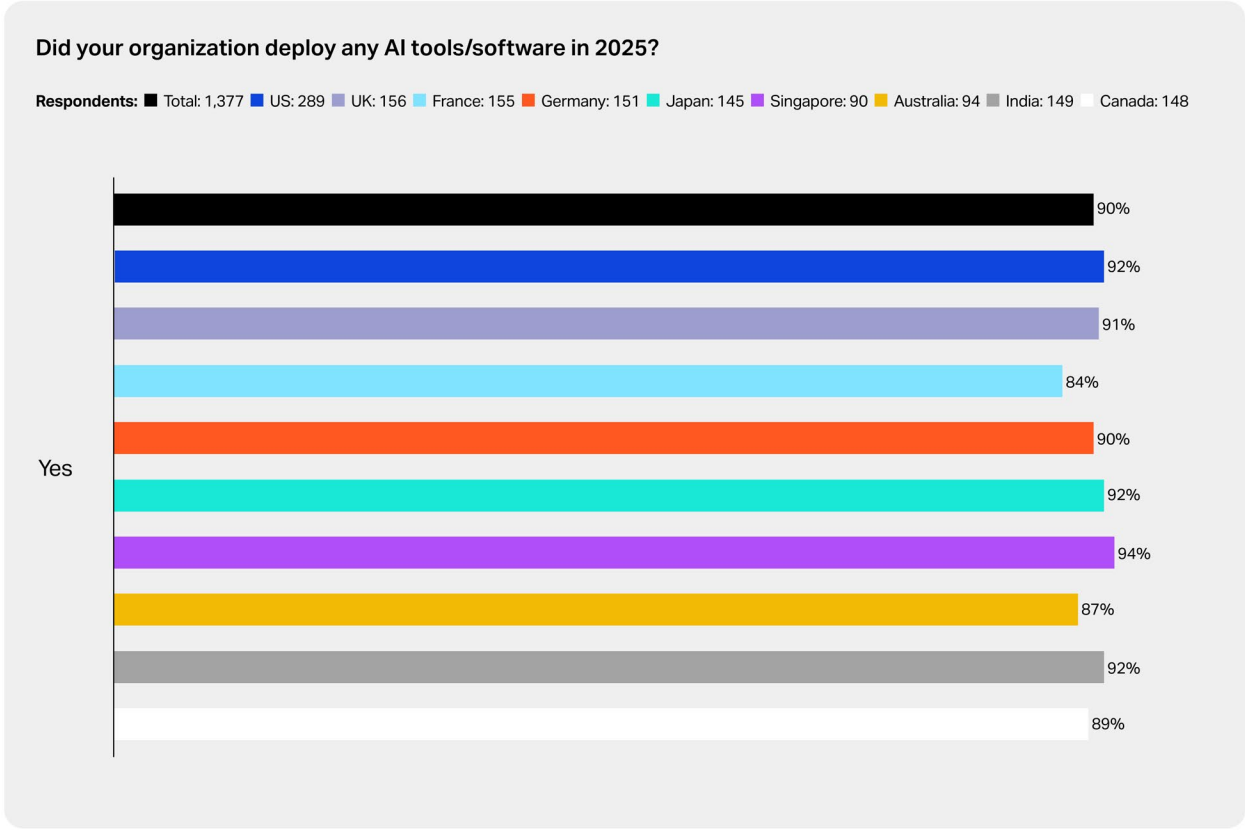
Data sanitization in the age of AI

Of our survey respondents, 90% had deployed AI in the past year, and of those, 99% destroyed at least some drives or devices as a result.

While many credit AI for improving data governance practices such as data classification and defining retention policies, there's no question that AI adoption is increasing the volume of data organizations generate, process, and store.

That's also placing additional pressure on device lifecycles.

At the same time, the external environment is shifting. Increased demand for memory and storage is contributing to rising costs for devices and drives. This makes it more difficult for organizations to plan hardware replacement—particularly if devices are being destroyed prematurely to mitigate perceived data risk.



The high cost of device destruction

The cost of a data leak or compliance failure is likely to be much higher than the cost of replacing devices.

This is leading many risk-averse organizations to destroy more devices than they need to.

However, this approach comes with its own cost.

In many cases, devices are still fully functional at the time of destruction. This applies to 43% of mobile devices, 35% of laptops and desktop PCs, and 44% of data center assets.

While destruction can reduce the risk of data recovery, it is not without limitations. Without rigorous oversight, factors such as chain of custody, tracking, and method effectiveness can introduce residual risk.

Cost and supply dynamics are also making asset refreshes more difficult to plan. With Gartner predicting a combined **130% surge in memory and SSD drive prices** by the end of 2026, organizations will need to balance the perceived security benefits of destruction against opportunity costs created by increasing financial and operational pressures.

Functional devices slated for destruction often can be redeployed internally, cascading to other use cases, departments, or personnel that can still excel with less than top-of-the-line technology. This extends device life and value, but only if concerns over data security are sufficiently satisfied.

The average age of devices at the time of destruction

Mobile devices (incl. smartphones and tablets)

2 years 4 months

Laptops and desktop PCs

3 years

Data center assets

3 years 8 months

Corporate devices are often physically destroyed before the end of their expected lifecycles.

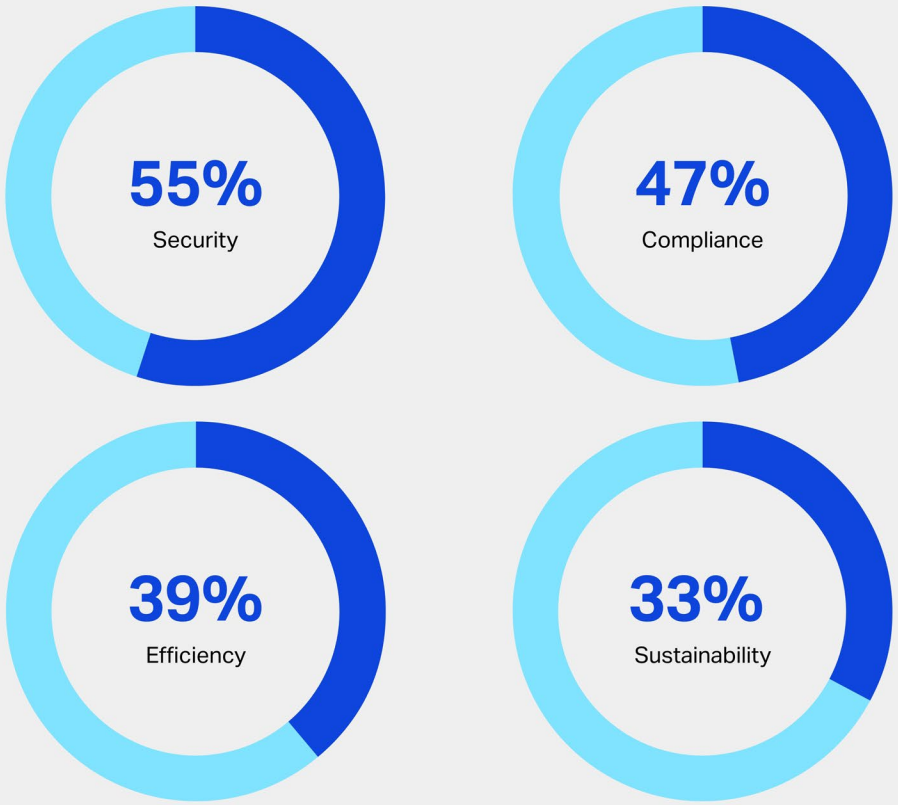
Security anxiety is winning over sustainability

Seventy-seven percent (77%) of respondents report a preference for reusing devices rather than destroying them. In addition, sustainability is a growing priority across regions, with 36% of organizations in North America, 38% in Europe, and 32% in APAC listing it as a key driver of data management changes.

However, sustainability is often outweighed by security and compliance concerns as well as a need for operational efficiency.

How much does security/compliance/efficiency/sustainability influence your organization's approach to processing end-of-life devices?

Percentage of respondents reporting each as a "major influence."



 |

Security anxiety is winning over sustainability continued

In the U.K., sustainability was a bigger priority, with 48% of organizations factoring it into their decisions.

When asked about barriers to advancing sustainability goals, 56% of organizations cite concerns around data security. This rises to 64% in the U.S. and 63% in Japan.

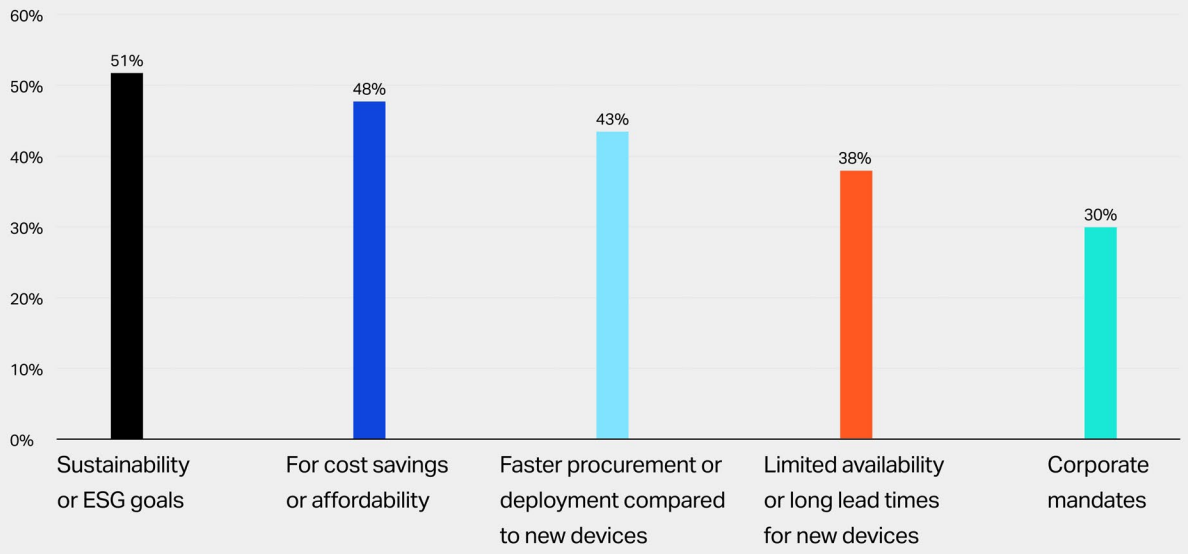
Legacy systems also play a role, with 53% of organizations reporting that they lack the technology to safely sanitize devices without destruction.

At the same time, only 37% cite lack of senior decision-maker support as a barrier—suggesting that change is not being blocked at the leadership level.

There is also a substantial secondary market within the enterprise space: 51% of respondents that purchased refurbished devices did so to support their organization's sustainability or ESG goals. Another 48% cited cost savings or affordability as a primary reason for purchasing used IT assets.

This points to an opportunity. Organizations are willing to improve sustainability outcomes but require greater confidence in their data sanitization processes to do so.

What are the main reasons your organization purchases refurbished devices?



Conclusion: Trust and confidence through best practice

Security anxiety can lead to costly decisions. For many organizations, the fear of data leaks is driving the destruction of devices that still have operational value.

While destruction can be appropriate in some cases, it is not always necessary—and can result in avoidable financial and environmental costs.

At the same time, organizations express a clear preference for reuse. Yet this preference is not consistently reflected in practice.

The issue is not intent—it is trust in process.

Only when organizations can consistently apply verifiable data sanitization methods and prove that data has been irreversibly removed can they reduce reliance on destruction. That shift enables more efficient, sustainable outcomes and helps organizations extract greater value from enterprise IT investments.

Research Methodology

Blancco commissioned independent research agency Coleman Parkes to survey 1,460 IT, compliance, and sustainability leaders across North America (U.S., Canada), Europe (U.K., France, Germany), and APAC (Japan, Singapore, India, Australia) from large enterprises (more than 5,000 employees) across regulated industries (BFSI (Banking, Financial Services and Insurance), Healthcare, Pharmaceuticals, Manufacturing, Technology, Automotive, Energy/Utilities, Transportation, Federal/ Government, Legal and Advisory). Fieldwork occurred in January and February 2026.

About Blancco Technology Group

Reduce Risk. Increase Efficiency. Be Sustainable.

Blancco Technology Group provides organizations with secure, compliant, and automated solutions that accelerate the transition to the circular economy. Each year, tens of millions of Blancco erasures allow top-tier organizations to protect end-of-life data against unauthorized access, safely redeploy data storage assets, and firmly comply with increased data protection and privacy requirements. Our precise device diagnostics help move used IT assets confidently into the circular economy, enabling enterprises, IT asset disposition (ITAD) vendors and recyclers, and mobile industry stakeholders to operate more sustainably.

Globally approved, recommended, and certified by governing and industry bodies around the world, Blancco is the industry standard in data erasure and mobile lifecycle solutions. With 40+ patented or patent-pending ideas, we continue to grow the number of innovative solutions global companies can rely on to accelerate operations, secure their data, and grow their businesses. Read more about us at **www.blancco.com**.