



RESEARCH STUDY

The Price of Destruction

Exploring the Financial & Environmental
Costs of Public Sector Device Sanitization

March 2022

Contents

- Introduction 3**
 - COVID-19 as Transformation Accelerator 3
 - Data Breach Disorder 3
 - A Global Sustainability Shift 4
 - The Implications 4

- Research Methodology 5**

- Survey Results & Discussion 7**
 - Regulatory Awareness and SSD Physical Destruction 7
 - The Financial and Environmental Cost of SSD Destruction 9
 - The Pursuit of Sustainable SSD Sanitization 10
 - The Pursuit of Secure SSD Sanitization 12
 - Methods of Sanitization 13
 - Data Security is Paramount 15

- Conclusion 16**

- About Blancco 17**

Introduction

In today's data-driven world, government and public sector agencies are responsible for managing, processing, and safeguarding some of the most sensitive—and potentially exploitable—information within society. While administrative structures differ globally, these agencies span public services, healthcare, education, transport, utilities, infrastructure, law enforcement, defense, and more. And, as in private industry, public sector data management is undergoing several profound shifts.

COVID-19 as Transformation Accelerator

In the U.K. alone, an accelerated rate of change in health and social care saw organizations compress three to five years of digital transformation into just 12 months, forcing through innovations to meet increased public service demands, new ways of working, the heightened need for resiliency, and access to information created by the pandemic.



However, some of the most promising areas for innovation also depend on some of the most sensitive data. Public sector organizations are responsible for citizens' Personally Identifiable Information (PII), Sensitive Security Information (SSI), as well as Critical Infrastructure Information (CII), to name a few. And all such data requires regulatory compliance and protection.

Data Breach Disorder

Perhaps not surprisingly, we are witnessing a shocking increase in data breaches and data breach costs. For example, in the public sector, the average cost of a breach surged by 78.7 percent globally between 2020 and 2021, from \$1.08 million to \$1.93 million. By comparison, healthcare data breach costs increased from an average total cost of \$7.13 million in 2020 to \$9.23 million in 2021, a 29.5 percent increase.

This leaves the public sector with an enormous responsibility to its citizens, especially as the importance of privacy and data protection is growing among both citizens and lawmakers.

Indeed, 69 percent of countries globally have data protection and privacy legislation in place. Laws such as the U.K. Data Protection Act (DPA), the EU General Data Protection Regulation (EU GDPR) and Japan's recent Amended Act on the Protection of Personal Information (Amended APPI, effective April 2022) direct organizations of all types on how personal information can be used and how it must be managed, distributed, and protected—including when data or data-bearing assets reach the disposal stage.

Within the public sector, additional regulations and policies govern the secure disposal of classified or secret data, as well as non-classified data, stored on data-bearing assets.

A Global Sustainability Shift

Worldwide, governments are also deeply involved in sustainability initiatives, establishing programs such as the [Greening Government Initiative](#) out of the U.S. and Canada, [Singapore's Green Plan](#), [Germany's Sustainable Development Strategy](#), and [France's Climate Plan](#). These are just a few at the national and international levels, with local government bodies launching additional programs. Many of these initiatives aim to address emissions, renewable energy, and waste reduction, raising the importance of having a sustainability focus within agency operations.

The Implications

So, what does all this mean?

Most government and public sector organizations store a great deal of data on solid-state drives (SSDs). These drives are in the cloud, in on-prem data centers, and used within various devices, such as desktops, laptops, or even multi-function printers. According to our global study of government agencies, whether because of a technology refresh, a data migration project, or other causes for decommissioning or retirement, internal government policies often (40 percent of the time) dictate these drives be physically destroyed at end-of-life to render classified or secret data permanently irretrievable.

However, there are other secure options of sanitization that are financially and environmentally more beneficial, particularly when compared to some physical destruction techniques. Non-destructive methods such as software-based data erasure or encryption are typically welcome for IT assets used for non-classified data. Yet, as results from our global survey show, even these SSDs are often destroyed out of perceived ease, an abundance of caution, and potentially, a lack of awareness of policy details allowing non-destructive options.

In the end, unnecessary SSD destruction increases IT operations and materials costs for fiscally constrained public sector organizations. It also fosters increased electronic waste (e-waste) creation during a global call for more prudent environmental stewardship.

This report aims to explore policies surrounding SSDs and the current methods of SSD sanitization used by government and public sector organizations around the world. It will also examine the relationship between maintaining a robust and resilient security posture and minimizing the environmental impact caused by the destruction of SSDs.











Finally, the study will highlight opportunities to revise, update, or inform SSD policy reform in a way that provides the robust security governments need while supporting regional and global sustainability goals.

Research Methodology











This report is based on an extensive survey of public sector decision makers across the globe. Respondents are evenly split across Public Services, Healthcare, Transport, Education, Infrastructure (e.g., transport and communications networks, waste disposal, water companies), and Utilities (all at 14 percent), and Law Enforcement and Defense (both at 8 percent).

The survey, undertaken by independent research company Coleman Parkes between December 2021 and January 2022, gathers data from government employees from nine countries: the United States (U.S.), Canada, the United Kingdom (U.K.), France, Germany, Japan, Singapore, India, and Australia. The countries represent the North America, Europe, and Asia Pacific regions in which Blancco operates.

Public sector departments represented by country

	 Avg	 Australia	 Canada	 France	 Germany	 India	 Japan	 Singapore	 UK	 US
Public Services	14%	17%	14%	14%	14%	14%	13%	14%	14%	14%
Healthcare	14%	17%	14%	14%	14%	14%	13%	14%	14%	14%
Education	14%	13%	14%	14%	14%	14%	17%	14%	14%	14%
Transport	14%	13%	14%	14%	14%	14%	13%	14%	14%	14%
Utilities	14%	13%	14%	14%	14%	14%	13%	14%	14%	14%
Infrastructure	14%	13%	14%	14%	14%	14%	13%	14%	14%	14%
Law Enforcement	8%	7%	8%	7%	7%	7%	8%	8%	7%	9%
Defense	8%	7%	8%	7%	7%	7%	8%	8%	7%	9%

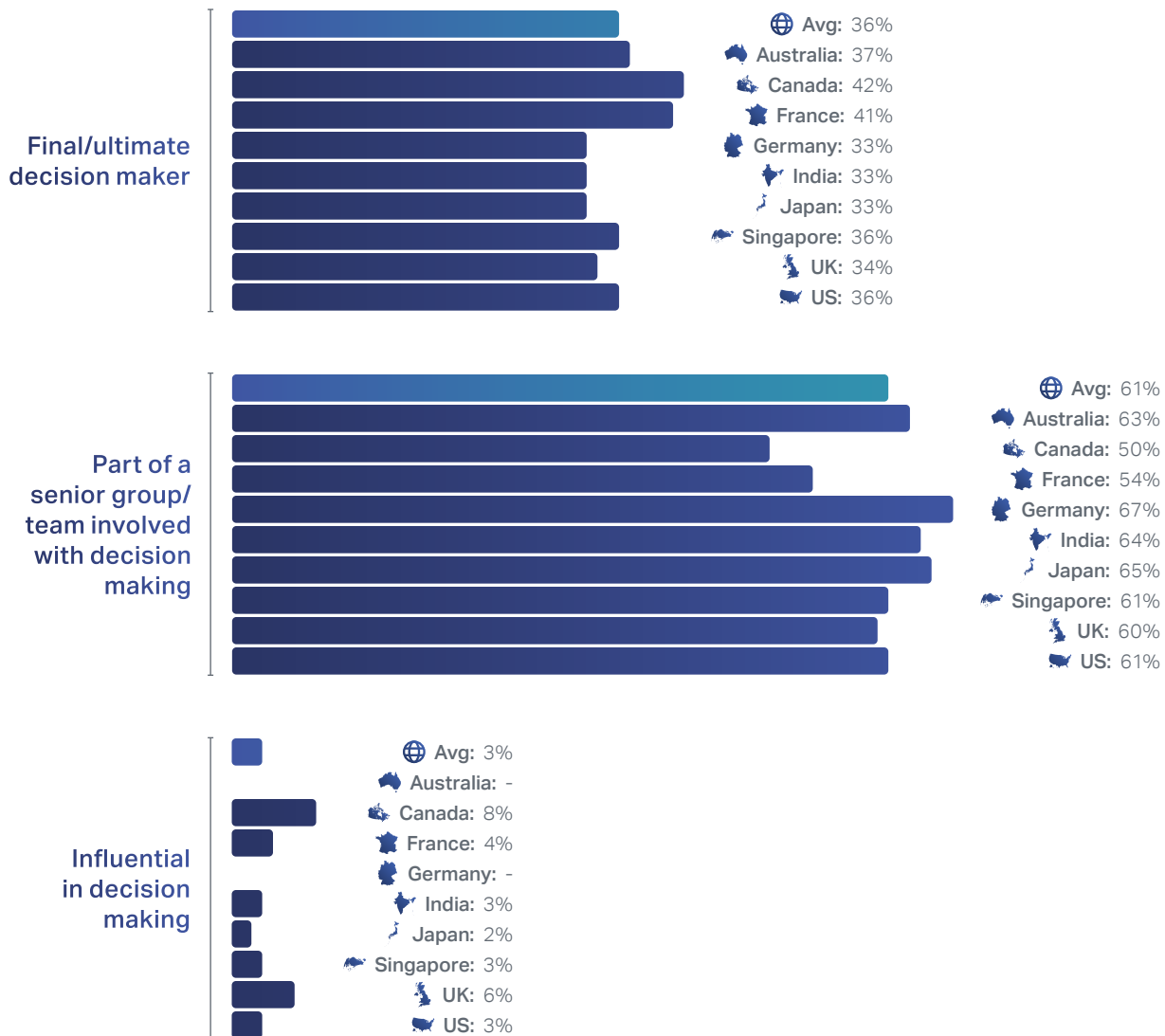
Base: All Respondents

 Total: 596
  Australia: 60
  Canada: 50
  France: 70
  Germany: 70
  India: 70
 Japan: 60
  Singapore: 36
  UK: 70
  US: 110

Those questioned comprise: Head of IT/IT Manager, Head of Compliance/ Compliance, Head of IT Operations, ITAM (IT Asset Manager), Head of IT Infrastructure/IT Infrastructure Manager, Chief Information Office (CIO), Chief Technology Officer (CTO), CISO (Chief Information Security Officer)/IT Security VP, Head of Risk Management, Chief Data Officer (CDO), and Data Protection Officer (DPO).

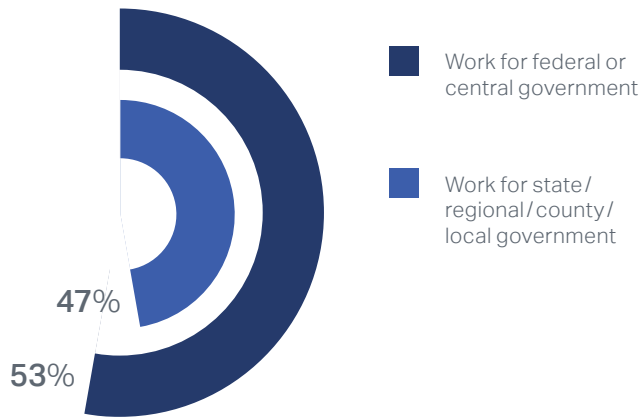
Ninety-seven percent of respondents are at least part of a senior group or team involved with decision making regarding SSD management policy and procedures. Thirty-six percent are the final or ultimate decision maker.

Level of decision-making responsibility regarding SSD management policy and procedures

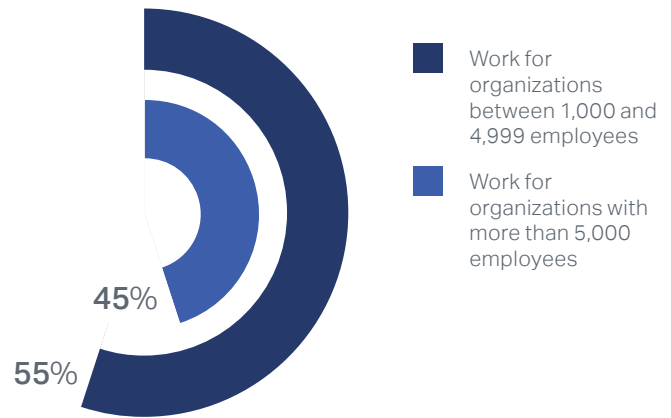


Seventeen percent are Heads of IT/IT Managers, and 11 percent held one of the following titles: Head of IT Operations, Head of Compliance/ Compliance Officers, IT Asset Manager, or Head of IT Infrastructure/IT Infrastructure Manager. Across almost all countries, the highest percentage of respondents falls into one of those categories.

Levels of government



Organization size



Survey Results & Discussion

Regulatory Awareness and SSD Physical Destruction

Understanding regulation awareness within the public sector for SSDs and SSD sanitization was a critical part of the study.

Respondents are familiar with the vast majority of data protection laws and sanitization guidelines, particularly those that are internationally referenced and viewed as most robust. These include the DPA and EU GDPR, the ISO 27000 standard, and NIST Media Sanitization Guidelines (NIST SP 800-88 r1). In fact, 100 percent of respondents have heard of the EU GDPR, the DPA, and ISO 27000. These references are now established and form a central part of working practice, so this comes as little surprise.

Indeed, the majority of respondents were well informed of their country's or region's respective data protection laws, including at a detailed level. However, in a few cases, awareness of specific requirements or process details was lower:

- While 69 percent of U.S. respondents know them in detail and 15 percent know some detail, a remaining 15 percent of IT leaders surveyed are "aware of only" when it comes to the internationally referenced NIST SP 800-88 r1 and do not know guideline details.
- Also in the U.S., 56 percent know in detail and 23 percent know in some detail, while the remaining 21 percent of respondents are "aware of only" when it comes to NIST 800-53 r5 Security and Privacy Controls for Information Systems and Organizations, revised in 2020.
- In the U.K., 93 percent of the respondents reported being aware of the EU GDPR and knowing it in detail, with one percent more (94 percent) having the same level of knowledge of the UK GDPR. However, only 47 percent stated they were both aware of and knew in detail the DPA 2018, which works alongside the UK GDPR.

The situation this creates is one in which a lack of awareness can lead to limited options, poor practice, or miscommunication of appropriate, secure, or efficient methods for handling data, particularly data that is categorized below "classified" or "secret."



Interestingly, in the U.S., the government regulation that had the greatest percentage (88 percent) of respondents reporting they are "aware of and know some detail" or are "aware of and know in detail" was the National Security Agency/Central Security Service (NSA/CSS) Policy Manual 9 12—a policy that advocates a non-reuse approach for media that contains classified information. It's understandable that this might be the most well-known of the national U.S. policies as it deals with the most critical information, but this widespread knowledge may also influence what U.S. IT leaders perform as standard practice when it comes to device sanitization and disposal overall, regardless of classification.

With the acceleration of both data privacy and protection laws, cyberthreats, the increased focus on environmental sustainability, and the rapid acceleration of data transformation, there is a need to consider all options allowed under governing regulations to create policies that fit today's government technology landscape.

Many of them, such as NIST SP 800-88 r1, provide non-destructive options for secure data sanitization, particularly for non-classified data. This is important to consider, especially as many countries continue to refine their data protection regulations.

Furthermore, for governments worldwide, non-destructive options provide an extra, immediate layer of security for the most sensitive of data when physical destruction is the only allowable choice.

The Financial and Environmental Cost of SSD Destruction

All together, our 596 respondents spend between \$12.8 million and \$17 million each year destroying SSD-based laptops, desktops, and servers along with loose drives, and nearly another \$40 million replacing the drives they've destroyed.

Of those surveyed, 55 percent worked for organizations having more than 1,000 and less than 5,000 employees and 45 percent for organizations having 5,000 employees or more. In both categories, organizations annually destroyed roughly one SSD for every three employees. This reflects common industry practice of refreshing technology assets every three to four years, with one-third of an organization's desktops and laptops being decommissioned annually. Data center SSDs and other loose drives across the organization also contribute to the number of devices decommissioned, but drive numbers vary based on whether an organization operates its own data center or has data in the cloud.

Respondents reported destroying an overall average of 1,433 SSDs annually. If we assume these are shredded onsite to NIST-compliant specifications, and that organizations include serialization (capturing serial numbers to identify and track each drive), a reasonable destruction cost is between US\$15-20 per drive, meaning each of our surveyed government and public sector organizations spends between \$21,495 and \$28,660 annually on drive destruction.

To replace a portion of the SSDs physically destroyed, respondents in our survey reported spending an average of \$65,235 for new SSDs, bringing the average total cost (for destruction and replacement) per respondent to between \$86,730 and \$93,895 each year. Multiply this by our 596 respondents, and destroying SSDs quickly surpasses tens of millions of dollars each year.











The public sector depends on tax revenue and is often beholden to its citizens and other government structures that provide budgetary oversight. While the cost to destroy, then replace, a single SSD may not seem like much, the government sector is typically one of the largest, if not the largest, purchasers of technology within a nation. Getting the best value is often a motivator when managing fiscal funds, and indeed, anywhere from 23 to 52 percent of organizations within a country believed that physical destruction was cheaper than data sanitization solutions that would facilitate reuse and longer device life.

Unnecessary SSD destruction increases IT operations and materials costs for fiscally constrained public sector organizations. It also fosters increased electronic waste (e-waste) creation during a global call for more prudent environmental stewardship.

However, the data shows that device destruction and replacement can cost even smaller governments millions of dollars each year. But this method of media disposal also incurs opportunity costs, as device life is cut short and redeployment, resale, and return options are taken off the table.

While precise numbers would require more information particular to each country, it's easy to see how device destruction costs quickly add up—and why this stage of asset management is worth revisiting.

Estimated total cost of drive destruction and new SSD purchases for survey respondents. Numbers are as reported or calculated per annum, per respondent, unless otherwise noted.

										
	Avg/Total	Australia	Canada	France	Germany	India	Japan	Singapore	UK	US
All Respondents	596	60	50	70	70	70	60	36	70	110
Avg yearly number of SSDs reported destroyed	1,433	1,348	1,385	1,748	1,506	1,456	1,331	1,292	1,478	1,316
Destruction costs at \$15-20 per SSD	\$21,495 -	\$20,220 -	\$20,775 -	\$26,220 -	\$22,590 -	\$21,840 -	\$19,965 -	\$19,380 -	\$22,170 -	\$19,740 -
	\$28,660	\$26,960	\$27,700	\$34,960	\$30,120	\$29,120	\$26,620	\$25,840	\$29,560	\$26,320
Avg yearly destruction costs in millions of USD for all respondents	\$12.8M -	\$1.2M -	\$1.0M -	\$1.8M -	\$1.6M -	\$1.5M -	\$1.1M -	\$0.7M -	\$1.6M -	\$2.2M -
	\$17.0M	\$1.6M	\$1.4M	\$2.4	\$2.1M	\$2.0M	\$1.6	\$0.9M	\$2.0M	\$2.9M
Avg yearly cost of new SSDs	\$65,235	\$58,334	\$65,100	\$66,857	\$70,715	\$49,000	\$51,500	\$51,945	\$68,786	\$84,455
Avg yearly cost of new SSDs for all respondents	\$39.1M	\$3.5M	\$3.3M	\$4.7M	\$5.0M	\$3.4M	\$3.0M	\$1.8M	\$4.8M	\$9.3M
TOTAL cost for all respondents to destroy and replace	\$51.9 M -	\$4.7M -	\$4.3M -	\$6.5M -	\$6.5M -	\$5.0M -	\$4.2M -	\$2.5M -	\$6.4M -	\$11.5M -
	\$56.1M	\$5.1M	\$4.6M	\$7.1M	\$7.0M	\$5.5M	\$4.7M	\$2.7M	\$6.9M	\$12.2M

The Pursuit of Sustainable SSD Sanitization

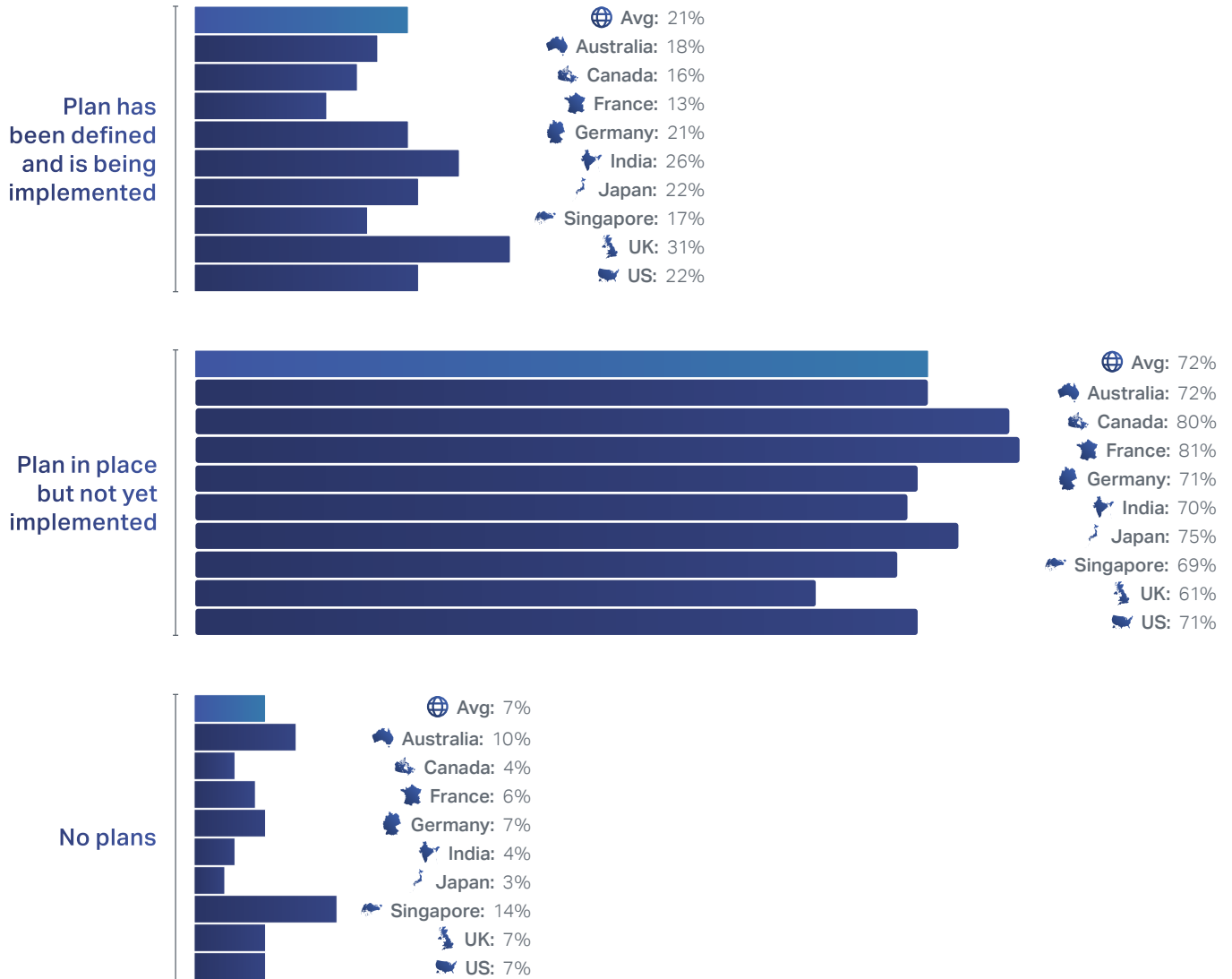
From an environmental standpoint, there are several outcomes to consider when ethically destroying any data storage asset: the working components from each device that can be harvested for reuse, the minerals and elements that can be extracted, the leftover waste that contributes to landfill, and the natural resources required to meet demand for new, replacement IT assets.

With global electronic waste (e-waste) called the “[world’s fastest growing domestic waste stream](#),” it may be no wonder that 93 percent of respondents have defined plans to reduce the environmental impact caused by destroying IT equipment. However, less than a quarter (21 percent) of the total are actively implementing those plans, with the U.K. (31 percent) and India (26 percent) having greater percentages of organizations in the implementation phase. Canada (16 percent) and France (13 percent) had the lowest percentage of respondents with plans in the

implementation phase, but also had the highest percentage of plans defined but not yet implemented (80 and 81 percent respectively).

Overall, most respondents reported at least having plans to reduce the harmful effects of destroying IT assets, showing that organizations are aware of the correlation between device disposal practices and environmental effects. Many, however, still need to take action to see plans become reality.

Status of organizational plans to reduce environmental impact caused by destroying IT equipment

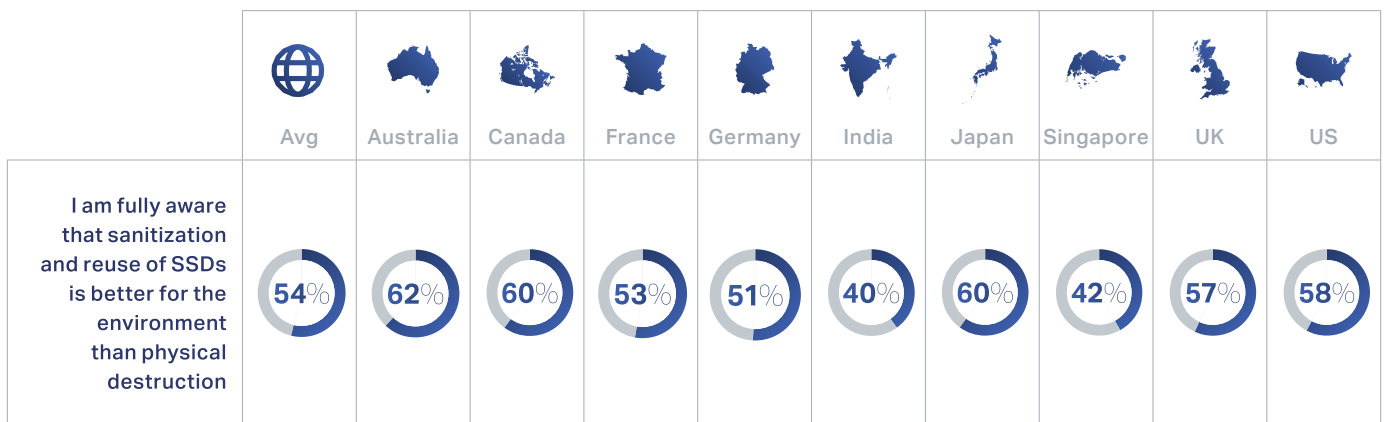


Ironically, while the nation of Singapore has made great strides in environmental initiatives, it had the most respondents with no plans at all to reduce the environmental impact caused by destroying IT equipment—14 percent. Singaporean respondents also reported a lower percentage of awareness (42 percent) of sanitization and reuse of SSDs as being better for the environment than physical destruction. This points to a need for

both industry and national leaders to understand and show the connection between the vast amounts of technology that governments use and the environmental goals and requirements that public sector organizations are striving to meet.

Globally, however, more than half of the respondents (54 percent) either slightly or strongly agreed that reuse of SSDs is better for the environment than physical destruction. These sentiments were more widely reported in Australia, Canada, and Japan, each of whom had more than 60 percent of respondents who agreed that reuse is better.

Percentage of respondents that chose "Slightly agree" or "Strongly agree" on awareness that sanitization was better than destruction.



The Pursuit of Secure SSD Sanitization

With so many public sector organizations exhibiting awareness of the need to rethink physical destruction, why are governments and public sector organizations destroying so many SSDs as par for the course?

Data security plays a big part. Physical destruction of SSDs is considered more secure than other data sanitization solutions by 46 percent of respondents globally and was as high as 53 percent in Singapore and 51 percent for the EMEA region.

The findings also indicate that physical destruction of SSDs takes place in many cases (40 percent of the time) because it is mandatory for classified data according to internal policies. Forty-one percent of respondents say it's mandated by law to physically destroy SSDs that contain classified data, so they destroy all SSDs "just in case."

However, the findings also uncovered a few surprises, which we briefly mentioned earlier: 38 percent of respondents believe device destruction to be cheaper than other methods. This grows to 52 percent of respondents in France. Another 38 percent globally and as much as half of the respondents in Singapore say they do not have the appropriate skills in house to use other sanitization methods.

Even more significant, however, is that almost a quarter (22 percent) are unaware of alternative methods of sanitization, such as certified data erasure or encryption.

What is quite surprising is 29 percent of Canadian respondents and 20 percent of Japanese respondents believe that physical destruction is better for the environment. It is a smaller number (15 percent) globally, but at a high level, sustainability is not a driving force for the destruction of devices. That motivation remains secure data management and ensuring that the data is rendered inaccessible.

Additionally, 35 percent of respondents globally believe there is no certified or approved vendor or solution that provides a sustainable option for secure data destruction, highlighting a missed opportunity. This issue is most prevalent in Singapore (47 percent) and India (41 percent). There is an opportunity for legislators and regulators to investigate and share the details of certified alternative providers that deliver compliant solutions.

Methods of Sanitization

We also discovered organizations may use multiple methods to sanitize their SSDs:

- **Cryptographic erasure** or encryption was indicated most often (by 89 percent of global respondents).
- **Software-based erasure** was used by about half the organizations (55 percent erased onsite; 45 percent erased offsite) to facilitate reuse.
- **Physical destruction of SSDs** alone was used by 60 percent of the respondents and physical destruction of IT assets that house SSDs was used by 48 percent.

Multiple selections were allowed.

In addition to the environmental and financial drawbacks of using physical destruction, it's important for organizations to realize that proper application is critical no matter what sanitization method is chosen:

- Properly applied from beginning to end, **encryption** is very effective. However, encryption keys must be securely stored and managed to thwart attacks. To be confident that all data on a drive is truly protected, users must be diligent in how and when they execute encryption processes. And, the less sophisticated the encryption, the shorter the shelf life as decryption technologies get stronger and more sophisticated.
- For **physical destruction** to offer true security, no data storage areas can be left intact and destruction methods must be appropriate to the asset.
- For **data erasure**, the use of accepted industry standards and verification of erasure are critical.

However, some processes for carrying out SSD sanitization are concerning. While it could be that organizations are combining methods with physical destruction, a worrying 78 percent of respondents said that they reformat drives to sanitize them. This was most common in India, with reformatting selected by 89 percent of the respondents from that country (this aligns with [Deloitte and Blancco private sector findings](#), which indicated a need for more education around proper data sanitization processes).

Unfortunately, formatting alone can still leave drives vulnerable during transport or storage, and much of the data can be recovered with forensics tools easily available online.

But these figures are staggering when compared with findings from the private sector in our previous *False Sense of Security* report: In that survey, 36 percent—half of what was found for government—reported using data wiping methods such as formatting, overwriting using free software tools or paid software-based tools without certification or physical destruction (both degaussing and shredding) with no audit trail.

That audit trail is critical for both private and public sector organizations. In the U.K. for example, NHS Digital was forced to record 393 lost or stolen devices over a 12-month period, despite having processed 319 of those laptops for disposal. The NHS Digital had no record of having disposed of those devices, so all of them had to be officially listed as lost, along with the data on them.

The verification and certification of data being rendered inaccessible is also incredibly important, particularly if used drives are to be reused either internally or externally or taken offsite. This is even more relevant given that SSDs containing classified data are more likely to be destroyed. This is no small matter, as between 37 and 45 percent of our respondents' devices, or the drives alone, are sent offsite for physical destruction.

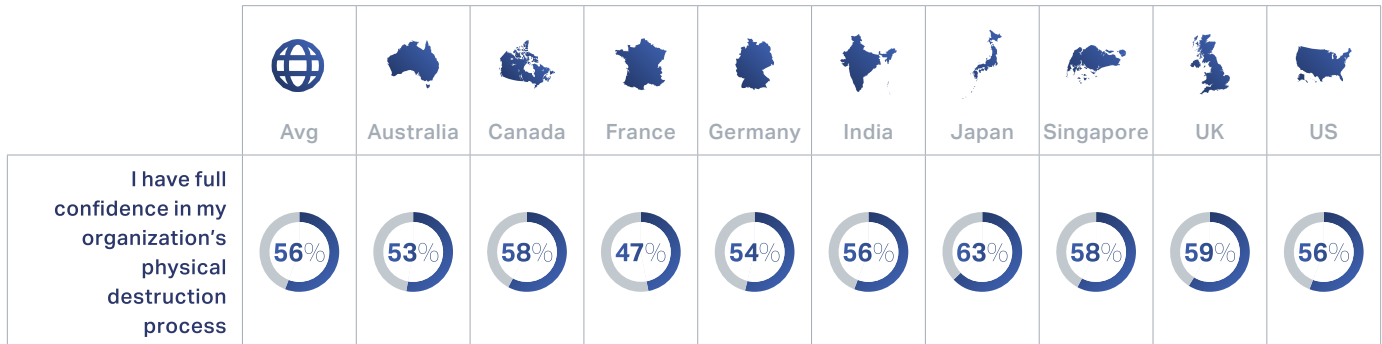
It's important to note that extreme diligence is required even when drives are being physically destroyed: On its own, and without qualifier, destruction of a drive does not guarantee that data is irretrievable. For instance, in the case of shredding, the larger shred sizes appropriate for hard disk drives may be inadequate to the task of destroying more densely populated data on an SSD. Yet, less than half (46 percent) of our global respondents sanitize SSDs of data before destroying them.



Data Security is Paramount

Ironically, while 46 percent of those surveyed stated that they physically destroy drives because it's more secure than other data sanitization solutions, only 13 percent strongly agree that they have full confidence in their organization's physical destruction process (43 percent slightly agree).

Level of confidence in destruction processes



For any non-physically destructive sanitization solution to meet the security needs of government organizations, it must be proven to prioritize data security. That means it must render data inaccessible against sophisticated, laboratory attempts at recovery to facilitate reuse or any other safe changes of hands. Typically, this is evidenced by a wide range of certified, third-party tests, including rigorous data recovery attempts. Subsequent verification and certification of sanitization must also be in place to assure policy makers and IT leaders that their data is indeed irretrievable. For non-destructive sanitization methods, this usually means receiving a certificate of erasure that documents the method of erasure used and other pertinent information.

While non-destructive data sanitization practices can often be adopted as a matter of agency policy, lawmakers can also reinforce the importance of certified data removal even if the final destination is destruction. For instance, following the loss of 18 hard drives destined for scrap, a [Japanese prefecture](#) recently revised its IT asset disposal procedures to protect against future data leaks by including witnessed, onsite data erasure before either reuse or destruction. In doing so, they reinforced data security for their most confidential data, sealed gaps in their chain of custody processes, and ensured secure reuse of preserved drives.

It is at this legislative or regulatory level that widespread change can occur—and where countries can align their public sector data security needs with local, national, and international sustainability goals.

Conclusion

Most government and public sector organizations are committing to sustainability improvements within their IT operations and are even testifying to having clear plans in place. But even so, less than a quarter of those organizations surveyed have pushed forward with actual implementation of said plans.

This results in government and public sector organizations globally still spending hundreds of millions of dollars on destroying and replacing perfectly functional IT equipment, including assets containing SSD storage. These costs consist of the actual cost of destruction, the costs of buying new replacement drives, and even the costs of entire systems when they are completely destroyed.

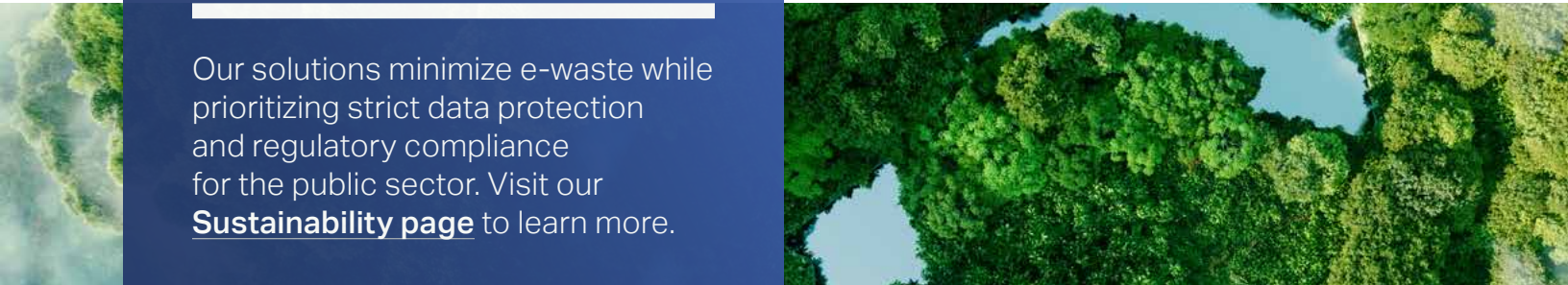
The main drivers behind physical destruction of these drives are a lack of awareness of alternate device sanitization practices and older policies not taking into account the latest advancements in data sanitization technology that provide purge-level data security without actual physical destruction.

In addition to this, there also appears to be an overreliance on incomplete data destruction practices, such as reformatting, which will significantly increase the risk for data breaches and additional related costs and penalties.

All together, our 596 respondents spend between \$12.8 million and \$17 million each year destroying SSD-based laptops, desktops, and servers along with loose drives, and nearly another \$40 million replacing the drives they've destroyed.

Governments and public sector organizations have always been under the spotlight when it comes to spending, but with global e-waste projected to nearly double by 2030 and persistent calls to more environmentally aware government practices, it is increasingly urgent that government organizations consider sustainable alternatives that extend device life, maintain lock-tight data security on end-of-life SSDs, and ultimately save public services millions.

A strong recommendation is to work for increased awareness and regulatory reform, revisiting both policy requirements and tenders for sustainable SSD sanitization when planning for extended asset lifecycles. These are worthwhile and well-timed initiatives to explore as agency and national policy makers seek to steward financial, environmental, and digital information resources entrusted to their care. Now is the time.



Our solutions minimize e-waste while prioritizing strict data protection and regulatory compliance for the public sector. Visit our [Sustainability page](#) to learn more.

About Blancco

Reduce Risk. Increase Efficiency. Be Sustainable.

Blancco Technology Group (AIM: BLTG) 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 public and private sector 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 35+ patented or patent-pending ideas, we continue to grow the number of innovative solutions global organizations can rely on to accelerate operations, secure their data, and grow their businesses.



Reduce Risk.
Increase Efficiency.
Be Sustainable.™