blancco

RESEARCH STUDY

A False Sense of Security

How gaps in data sanitization knowledge are leaving global enterprises open to breaches, compliance failures and lost profits

November 2019

rev 2019.11

Table of Contents

About the Report

This report is based on an extensive survey of:

- 1,850 senior decision makers with job titles of Head of Compliance, Chief Financial Officer, Finance Director, IT Asset Manager, Chief Information Security Officer, IT Security Vice President, Data Protection Officer and Head of Operations
- From enterprises across the world, including USA/Canada, U.K., Germany, France, Japan, India, Singapore and Australia
- Government, technology, finance, healthcare, pharmaceutical, defense, legal, manufacturing, energy, transportation and advisory
- Enterprises with over 5,000 employees

The research was undertaken by independent research company Coleman Parkes Research in August 2019.

Figure 1.

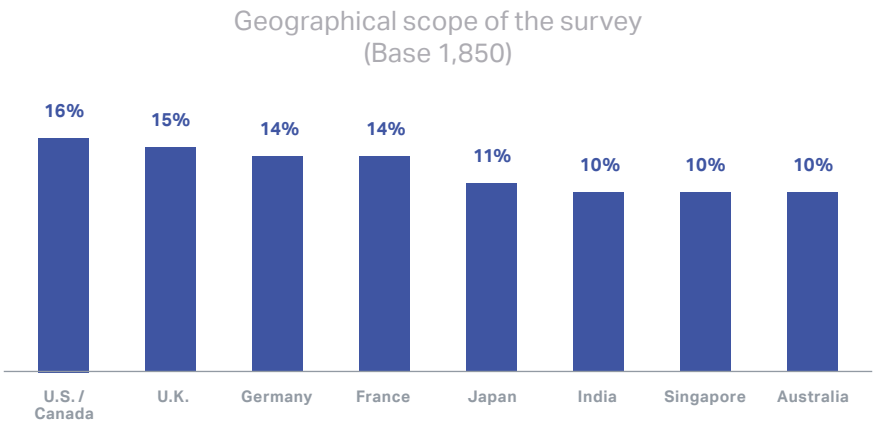
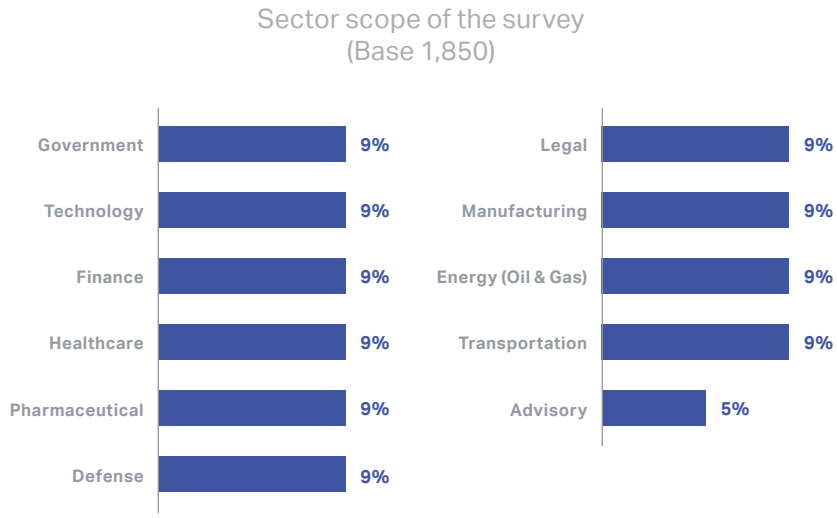


Figure 2.



Executive Summary

It's been a busy time for data protection.

The accelerated growth in data privacy regulations such as the GDPR in Europe and CCPA (California Consumer Privacy Act), along with the increase in widely reported data breaches and the resulting fines, means that data privacy and security and regulatory compliance are high-profile issues that raise concerns for enterprise organizations across the globe.

Those growing concerns have pushed organizations to invest 10.5 percent more in security in 2019 than the previous year to protect the integrity of their data throughout its lifecycle. Gartner—the world's leading research and advisory company—has also now placed data sanitization at the start of the upward "Slope of Enlightenment" in three of its reports—the Hype Cycle for Data Security, 2019; Hype Cycle for Privacy, 2019; and Hype Cycle for Endpoint Security, 2019.[1]

According to Gartner, these concerns—along with "the ever-expanding capacity of storage media and volume of edge computing and IoT devices—is making robust data sanitization a core C-level requirement for all IT organizations." Data sanitization is no longer viewed as a "nice-to-have" element of a wider data management practice — it's a necessity. Enterprises must have effective policies and processes in place to securely manage what happens to data stored on any device at its end-of-life, as well as procedures to sanitize data through life, to meet retention requirements and data minimization best practices. They must become data stewards.

Failing to ensure that devices are clear of customer, commercial, employee and other sensitive data leaves businesses open to potential breaches and noncompliance—both of which carry significant reputational and financial risks.

And yet, in our research carried out with Coleman Parkes into the attitudes and methods of data sanitization of 1,850 of the world's largest enterprises, we found that a surprising and worrying 36 percent—more than one in three—are taking considerable risks with the way they sanitize data at end-of-life.

These risks include:

- ☑ Using inappropriate data removal methods
- ☑ Keeping large stockpiles of out-of-use equipment within the company and not dealing with them within a suitable time frame
- ☑ Failing to maintain a clear chain of custody with an appropriate audit trail of an asset's end-of-life journey (including during transportation to an offsite facility)

[1] "Gartner Says Global IT Spending to Grow 3.7% in 2020." www.gartner.com/en/newsroom/press-releases/2019-10-23-gartner-says-global-it-spending-to-grow-3point7-percent-in-2020. 23 October 2019.

[2] Gartner Hype Cycle for Data Security, 2019, Brian Lowans, 30 July 2019; Gartner Hype Cycle for Privacy, 2019, Bart Willemsen, 11 July 2019; Gartner Hype Cycle for Endpoint Security, 2019, Dionisio Zumerle, John Girard, 31 July 2019.

Executive Summary

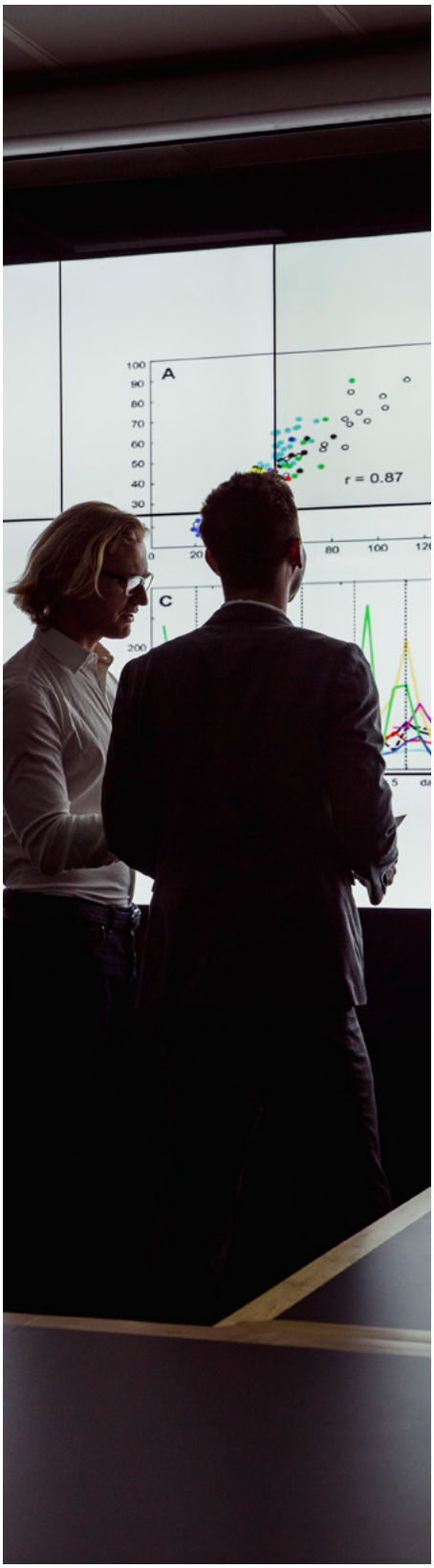
In a bid to educate the industry on this complex and important area, Blancco is now publishing the research as a three-part series of reports, identifying and exploring several issues around security, data policies and corporate social responsibility (CSR).

This first report examines how enterprises are dealing with data erasure, especially at the end-of-life stage. The report investigates the cost of destroying IT assets as well as the current misconceptions that prompt so many decision makers to mistakenly choose inadequate approaches. The report also offers advice on best practice for moving forward. Follow-up reports will focus on the difference between data policies versus data realities and the highly topical issue of CSR.

The research shows that, in many enterprises, there is a special focus at device end-of-life on physically destroying devices. Enterprises often feel that this is enough to protect against sensitive data on end-of-life assets falling into the wrong hands. However, physical destruction also has significant drawbacks. Enterprises might be deluding themselves into thinking that devices are being securely sanitized—either internally or by third-party vendors—when in fact they are not.

We hope you find this report useful as you develop or redesign your own device end-of-life data sanitization policies.

Introduction



Global enterprises face a perplexing dual challenge when it comes to that most valuable resource in today's increasingly digitalized economy: data.

Enterprise data volumes are growing exponentially, and new technologies like IoT devices and AI will accelerate this growth well into the future.

The sheer amount of data that enterprises are responsible for is exploding—and so too is the number and variety of devices that this data reside on. From data centers to desktops, laptops to mobile phones, tablets to drives, large enterprises own and use an expanding range of devices.

There is no sign of either device numbers or data volumes slowing down any time soon.

And while new technologies enable flexibility and encourage innovation, they can also cause headaches for enterprises from a data management and security perspective. For example: what happens to the data that resides on a device when it becomes obsolete or when the employee who uses it leaves the business?

Our research finds that the majority (96 percent) of the world's largest enterprises have a data sanitization policy in place and have also adopted a variety of approaches to remove data from end-of-life devices. While this is heartening and shows their commitment, when we dig beneath the surface, the situation is rather alarming.

A worrying number of enterprises report using what they believe to be the most secure and auditable methods of data sanitization to remove data at end-of-life. However, upon closer inspection these methods are, in fact, highly unsecure. They include:

- Data wiping methods such as formatting
- Overwriting using free software tools (e.g., KillDisk/DBAN)
- Physical destruction (both degaussing and shredding) with no audit trail
- Overwriting using paid software-based tools (without verification/certification)

Taking action to remove data at end-of-life is a step in the right direction. However, these methods only provide a small level of protection. The choice of these methods shows a lack of awareness around the drawbacks of some of these options and a shortage of robust data sanitization competency. But what's of particular concern is that some enterprises report not sanitizing at all, leaving them wide open to potential attacks.

The research also finds that 17 percent of enterprises use physical shredding or degaussing (either with or without audit trails) for end-of-life devices. This accounts for at least 1,650 devices per year per company, as identified in the research.

However, shredding does not necessarily provide a true, certified audit trail that spans the full chain of custody lifecycle. Furthermore, there is no evidence to suggest that companies check that their shredding process is carried out to the recommended two millimeter or less levels for SSDs. And there is no verification method for them to prove if they have done so.

Introduction

Part of the problem is that physical destruction is sometimes seen as being cheaper than software-based sanitization. This a misconception, as it can be much more cost-effective to use software-based erasure, especially when your security policies dictate media must be sanitized onsite. Physical destruction is also potentially harmful to the environment and completely blocks any possibility of the device being reused, whereas data erasure software often allows businesses to recoup the value of their devices.

What is also concerning is that enterprises often stockpile devices for future sanitization. Many enterprises do not even have a clear view of how many devices might be lying around in offices, data centers or storage rooms. This creates an additional layer of risk, particularly as many security breaches occur internally.

We discovered that senior security decision makers are concerned when it comes to data on end-of-life devices. However, despite understanding the risks involved, many adopt an inadequate approach to protecting their organization and fail to put in place and enforce an effective and comprehensive process across the business.

Here are some steps for enterprises to follow to get back on track with their data sanitization responsibilities:

1. Select a smart approach to data sanitization that minimizes risk with a clear and certified process
2. Embed this approach into the fabric of the business through clear and regular communication across all departments
3. Improve awareness of the volume and different types of end-of-life devices that need to be dealt with
4. Focus on minimizing the risk to the business of data loss and breach through end-of-life equipment management

With new technology arriving in the workplace every day, and businesses and individuals alike constantly generating new data, the issue of data sanitization is a pressing one. Enterprises that take data risks seriously are safeguarding their business and putting in place a stable and secure environment in which to operate, innovate and grow—now and into the future.

Part 1: Data Sanitization Today

How do enterprises deal with end-of-life devices?

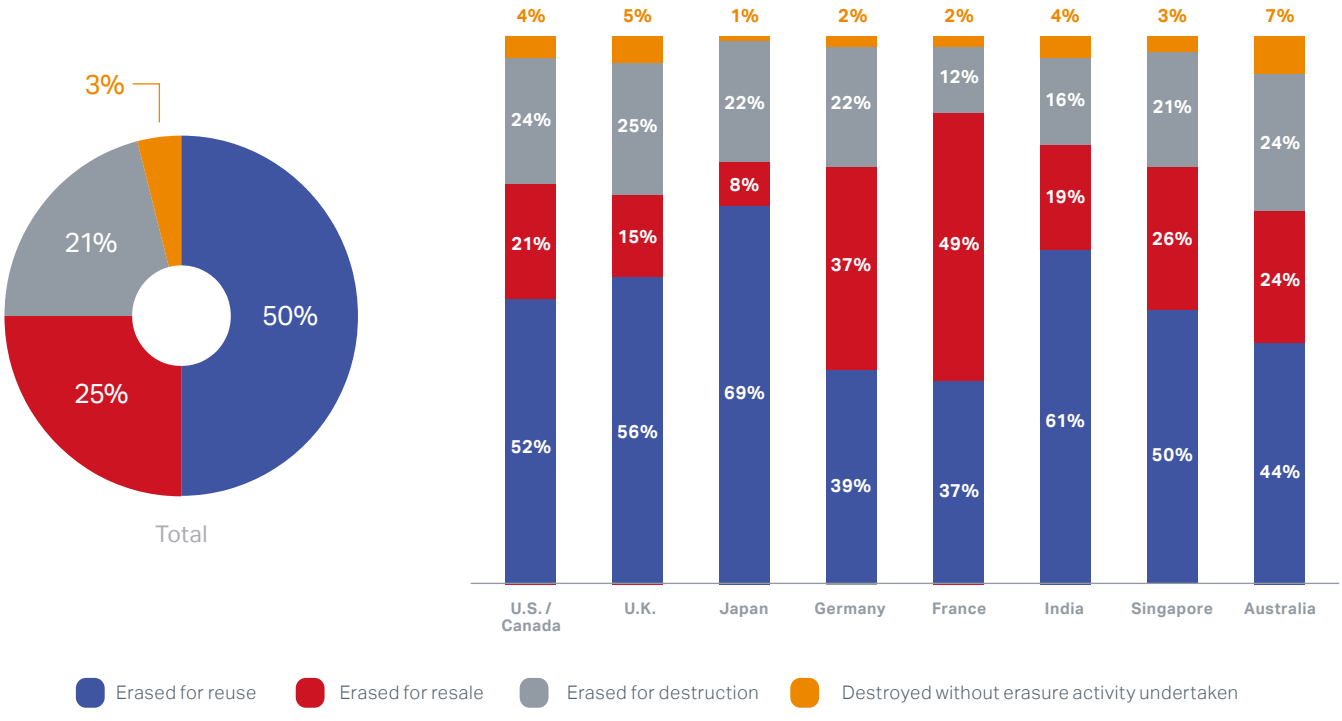
It's encouraging to see that most large enterprises (96 percent) have a data sanitization policy in place. Even among that small proportion with no policy yet, the main reason for not having one is geopolitical uncertainty (including Brexit), as opposed to not understanding that one is required. Where a policy exists, it is almost always (92 percent of the time) part of an overall reuse and disposals policy, demonstrating that businesses are aware of the importance of managing their devices and are trying to do so in an environmentally friendly manner.

When asked how they typically manage end-of-life equipment, three quarters (75 percent) of all enterprises (77 percent in Japan and 78 percent in India) erase equipment for reuse or resale. This is a positive for the environment, ensuring devices are not simply discarded never to be used again. Most of the remaining enterprises (21 percent) erase devices with the plan to destroy them, which is certainly not as green and is not necessary today, given the variety of software-based sanitization methods available which then allow for greater device reuse.

A small number—three percent—destroy their devices without any form of previous erasure activity being undertaken. If this physical destruction follows best practices, it can be a safe way to destroy data, but if an audit trail is missing, enterprises could be opening themselves up to major data breaches.

Figure 3.

How end-of-life equipment is typically managed (Base 1,850)



Are enterprises following best practices?

There is strong evidence that many enterprises are not using appropriate, best-practice methods when removing data from their end-of-life devices. A third (36 percent) of senior decision makers report that they are using:

- Data wiping methods such as formatting
- Overwriting using free software tools (e.g., KillDisk/DBAN)
- Physical destruction (both degaussing and shredding) with no audit trail
- Overwriting using paid software-based tools (without verification/certification)
- No method at all to sanitize data (a small but very worrying 4 percent)

Figure 4.

Proportion of companies using shredding or degaussing

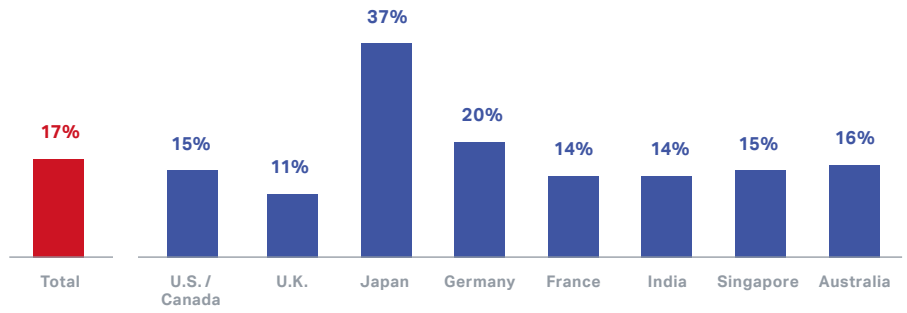


Figure 5.

Average number of known devices destroyed per annum per company – by device type

	MOBILE DEVICES	LAPTOPS AND DESKTOPS	SERVERS AND DATA CENTER STORAGE	LOOSE DRIVES	TOTAL ALL DEVICES
Total	435	404	339	475	1,653
U.S. / Canada	395	415	395	448	1,653
U.K.	489	417	481	506	1,893
Japan	513	373	133	458	1,477
Germany	434	452	456	602	1,944
France	488	402	399	399	1,688
India	334	417	338	463	1,552
Singapore	439	375	276	486	1,576
Australia	269	391	395	392	1,447

The first four methods lead to some form of data cleansing, but they are far from fully secure and can leave businesses open to potential data breaches and contravention of their policies as total sanitization is not ensured. The last, having no method to sanitize data, is highly dangerous, as leaked sensitive information can quickly ruin a company's reputation.

As many as 17 percent of companies are currently using physical destruction as one of their key ways to manage end-of-life equipment, accounting for at least 1,653 known devices per year per company.

It is clear that physical destruction can be costly, and if not undertaken following best practice methods with an associated audit trail for each device, can put data and the company at risk.

Part 2: A Focus on SSD Drives

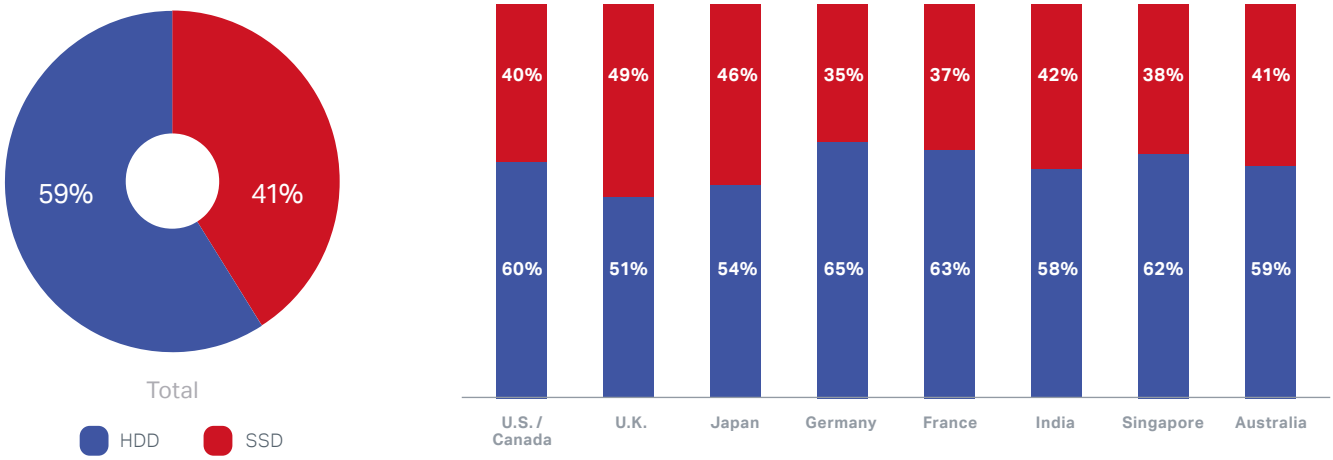
Sanitizing end-of-life solid-state drives (SSDs) is considerably more complex than sanitizing other devices. SSDs are becoming almost as common as hard disk drives (HDDs) in the overall corporate infrastructure. However, there are significantly greater security challenges that must be addressed to ensure SSDs are correctly processed to achieve data sanitization. SSDs can be used on their own in a device such as a laptop but are also now frequently used alongside HDDs in the same machine. These mixed environments—containing very different types of storage—can introduce confusion over how to address data erasure.

Are enterprises primarily using HDD or SSD devices?

The U.K. has an almost equal proportion of each drive type being destroyed, but across all geographies responding, more HDDs are being destroyed, accounting for 59 percent of destructions compared to 41 percent for SSDs. But with such high figures for both, our research suggests that businesses need to think carefully about how they deal with end-of-life HDDs and SSDs.

Figure 6.

Proportion of HDDs versus SSDs destroyed per annum (Base 316)



Survey Results & Discussion

Why focus on these devices?

According to Transparency Market Research's latest SSD research, the global SSD market is expected to reach USD $229.5 billion by 2022, more than the entire 2018 gross domestic product of Iraq, Peru or Greece.

With the rapidly growing popularity of SSDs due to their increased storage capacity (five or six times that of a typical HDD), lower and faster read/write rates, support for more IOPS (input/output operations per second) and lower power usage, the need to dispose of these devices appropriately at end-of-life is becoming more important.

How are enterprises tackling end-of-life sanitization for HDDs vs. SSDs?

Degaussing is not an effective sanitization method on most flash-based memory devices, including SSDs. This is because SSDs use integrated circuit (IC) assemblies (interconnected flash memory chips) to store data instead of storing it magnetically. SSDs are also not fully destroyed by standard hard disk drive shredders, leaving the possibility for data to be recovered.

Our research finds that a fifth (22 percent) of all enterprises (33 percent in U.S./Canada and the U.K.) do not have a different process for dealing with SSDs compared to HDDs. But shredding needs to be two millimeters or less to be effective for SSDs, according to the U.S.'s National Security Agency (NSA), while most disk drive shredders will only shred to six millimeters.

Companies must ensure that they are shredding devices to at least the minimum recommended standard or data could be accessed. Otherwise, they are running the risk of not having all the data appropriately sanitized, and noncompliance with industry standards. In fact, it is essential that every enterprise organization's data sanitization policies support the same high security level of sanitization for both HDDs and SSDs.

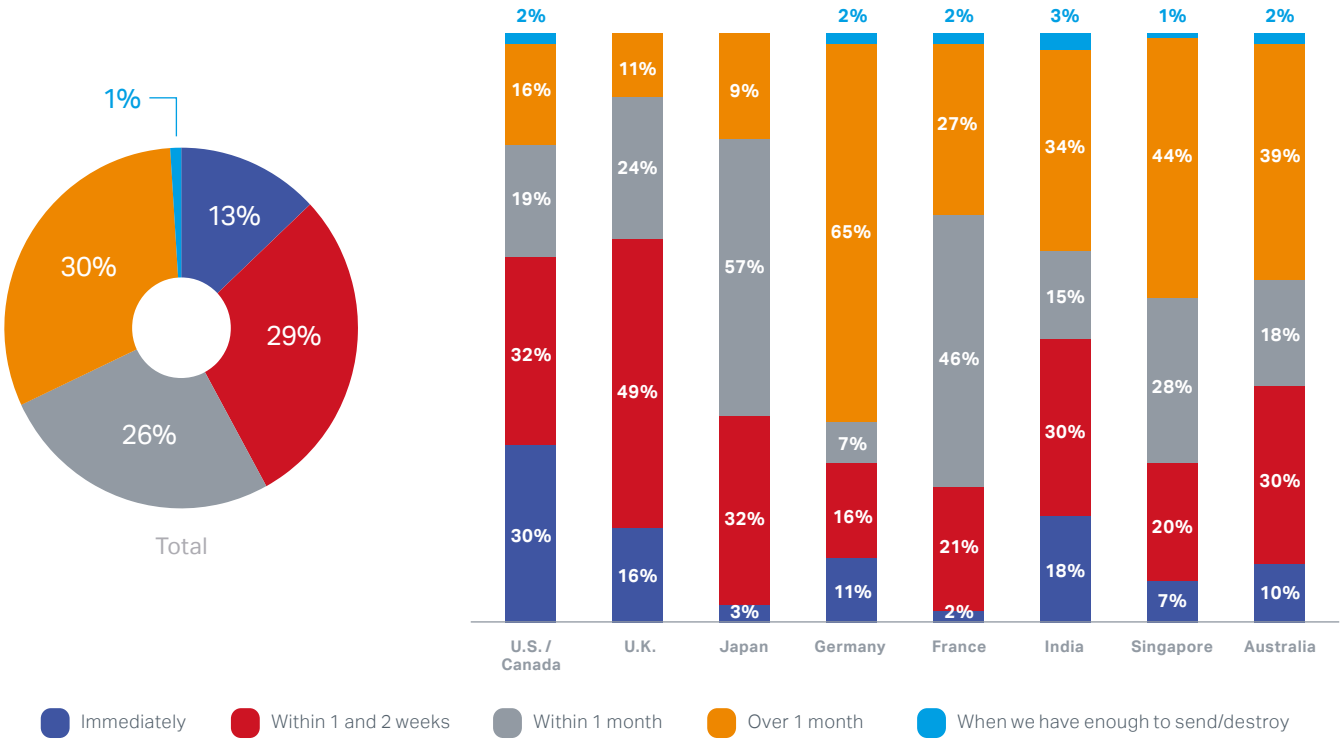
Part 3: On the Backburner: Stockpiled & Neglected Devices

We've seen that many companies are physically destroying devices in ways that could lead to a data breach if not tracked through the full device chain of custody. But 80 percent of all organizations (87 percent in France and 85 percent in the United Kingdom) also have a stockpile of out-of-use equipment totaling around 400,000 items, or an average of 272 devices per company, sitting in storage. Given the number of devices being destroyed, this is a conservative figure, and given the low numbers of stockpiled drives and devices reported, there is evidence to suggest that enterprises are not fully aware of the whereabouts of all the devices within the company.

In addition, not only are enterprises stockpiling, they are also leaving devices unused for some time, adding to the risks of data breaches and lost data. Only 13 percent of companies erase end-of-life equipment immediately, with companies in the U.S./ Canada performing best (30 percent). Overall, 57 percent of companies take longer than two weeks before erasing devices. Couple that with the fact that 18 percent of devices are left somewhere within the company with no action, many end-of-life devices are neglected. This highlights a huge security issue and one that enterprises should deal with immediately.

Figure 7.

Time between decommissioning and erasure (Base 1,800)



The overconfidence effect

What's the most alarming is that decision makers do understand that having end-of-life devices stockpiled or not dealt with effectively incurs additional security risk. Seventy-three percent agree that the large volume of different devices at end-of-life leaves the company vulnerable to a data security breach (87 percent of those in Japan shared this view). Sixty-eight percent are very concerned about the risk of a data breach with end-of-life equipment.

And yet most are comfortable with how they are dealing with the issue and not making sure they have robust data management and security processes in place. Sixty-nine percent have full confidence in the secure erasure for data sanitization within the organization. Seventy-four percent have full confidence in the company's physical destruction process.

These results show that senior leaders' overconfidence is leaving them blind to the gap between what they are doing to mitigate the risks of a data breach or data being recoverable—and what constitutes best practice.

Enterprises can mitigate these risks by taking a strategic approach to policy development for data sanitization and avoiding unnecessary delays by investing in automated methods that provide full data sanitization as well as verification and certification that the process has been completed properly. Destruction by shredding or degaussing is appropriate if the risks are fully understood and appropriate audit trails and certification is assured. But there is evidence to suggest that the vulnerabilities are far from appreciated and many enterprises are running unnecessary data breach risks, most notably with SSDs, at a time when data management should be at the forefront.

Part 4: The Cost of Misplaced Perceptions

What's the best way to prevent a breach, according to decision makers?

When questioned about which methods provide the best way to prevent a data breach, 44 percent of decision makers selected cryptographic erasure/encryption. Cryptographic erasure means erasing the encryption key of a self-encrypting drive. The encryption algorithm must be a minimum of 128 bit for the process to be successful. While the data remains on the storage device itself, by erasing the original key, the data is difficult to decrypt. Thus, the data is rendered unrecoverable.

But like any data sanitization method, there are advantages and disadvantages to using cryptographic erasure. Cryptographic erasure is an ideal solution when storage devices are in transit or require a fast erasure process (e.g., before internal deployment within the same company or in environments in which data must be obfuscated quickly). However, the process relies heavily on the manufacturer, where implementation issues could occur.

Additionally, users can impact the success of cryptographic erasure through human error and broken keys. It's only valuable for drives that are encrypted by default, and it doesn't include data destruction to fully remove data—meaning recovery is sometimes

possible. Even when a primary cryptographic erasure key is deleted, there are often more backups to that key, and the cryptographic erasure process doesn't meet regulatory compliance requirements if it doesn't include verification and certification as part of the process.

Many enterprises are using other methods to sanitize their data. Only a slightly smaller proportion—38 percent—placed shredding in their top three approaches, with 12 percent ranking it number one. Thirty-seven percent selected degaussing within their top three options, with 11 percent ranking it first.

While shredding and degaussing can be appropriate methods to sanitize data, it is critical to follow best practice methods and maintain a full chain of custody for each device. Enterprises must also ensure a different process is used for SSDs and hybrid HDD/SSD devices than for traditional HDD devices. Failure to do so puts companies at risk.

Thirty-four percent of respondents ranked drive (re)formatting as one of their top three options for providing the highest protection to a data breach, seemingly unaware that this does not remove access to the data entirely. Companies in the U.K. (22 percent) and France (17 percent) rated this option first.

All three of these methods could put companies at risk of a data breach if best practices are not followed. It's clear that many companies are working under the misconception that the methods they are using are more fit-for-purpose than they are. Physical destruction, either degaussing or shredding, is only an appropriate method of data sanitization if managed and audited properly, with a fully secure and visible chain of custody. Other methods, in particular drive reformatting, expose companies to high risks of a data breach.

Figure 8.

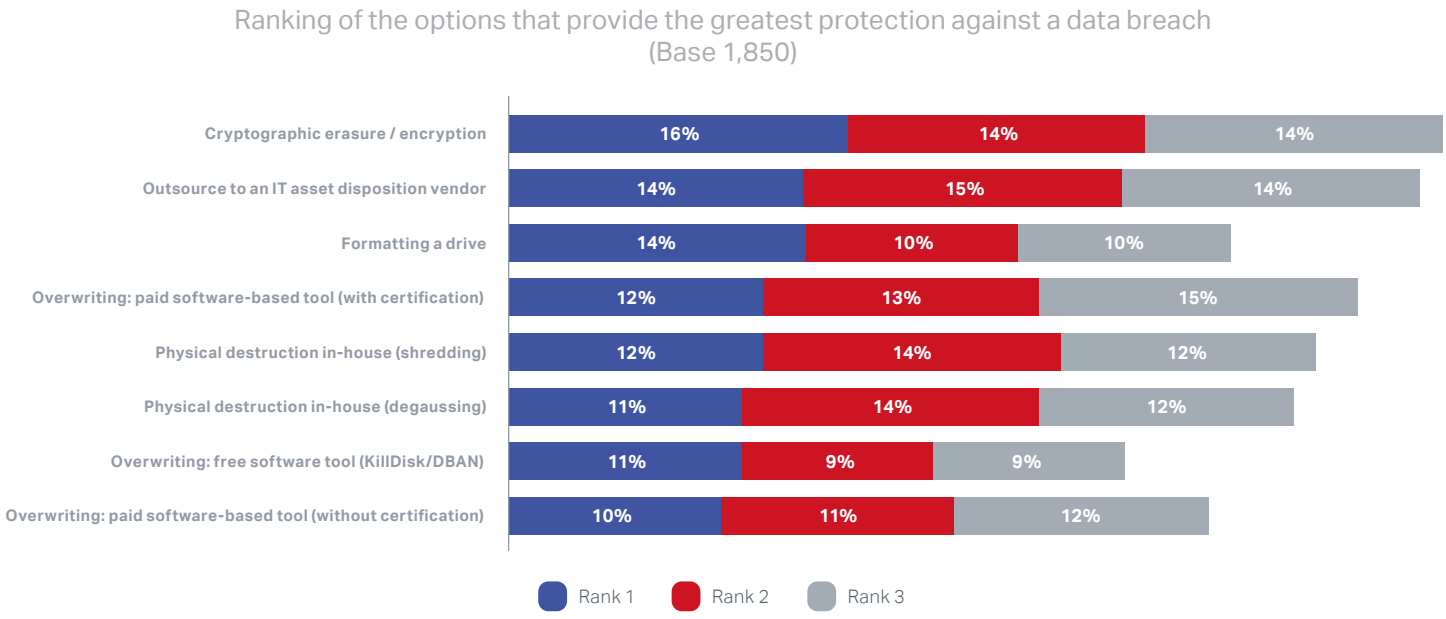


Figure 9.

Top reasons for physically destroying unfunctional or end-of-life equipment (Base 319)

	IT'S MORE SECURE THAN OTHER DATA SANITIZATION SOLUTIONS	IT'S EASIER AND QUICKER THAN USING OTHER DATA SANITIZATION SOLUTIONS	DATA SANITIZATION IS UNDERTAKEN WHEN WE DESTROY THE EQUIPMENT	IT IS CHEAPER THAN OTHER DATA SANITIZATION SOLUTIONS	IT'S BETTER FOR THE ENVIRONMENT
Total	52%	50%	48%	45%	39%
U.S. / Canada	39%	55%	39%	52%	30%
U.K.	48%	58%	67%	45%	55%
Japan	63%	63%	59%	49%	55%
Germany	49%	33%	25%	31%	29%
France	54%	34%	40%	46%	29%
India	42%	54%	42%	38%	46%
Singapore	61%	54%	71%	57%	29%
Australia	48%	48%	41%	38%	28%

1. Misplaced Trust

When asked why their company physically destroys unfunctional or end-of-life equipment, 52 percent of decision makers (63 percent in Japan), believe it is more secure than other sanitization methods. In the case of end-of-life devices, this is a misconception as it may not guarantee complete data sanitization, especially for SSDs. These companies may be running the risk of data breaches and data loss. For equipment that is no longer functional, destruction is the best available method since it cannot be erased.

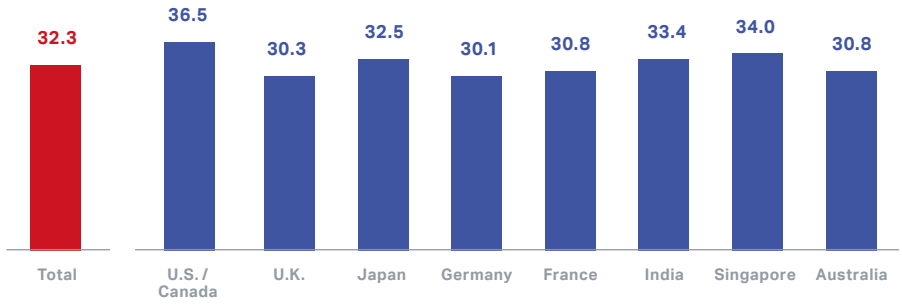
2. Cost Misconception

Half of companies (63 percent in Japan, but only one third in Germany) believe that physical destruction is easier and quicker than other sanitization methods. This misconception fails to take into account the time that proper destruction takes: on average, enterprises spend 32.3 hours per month destroying devices—that's one person spending 16 days every year, destroying equipment. Our two decades of experience in simplifying, automating and scaling data erasure tells us that automation using software-based erasure can slash the number of hours spent on performing sanitization in-house.

We also understand the hidden costs associated with physical destruction. This survey provides clear evidence that many senior leaders do not fully understand what destruction or storing useless IT hardware is costing their business. When questioned on the average cost of the destruction, 45 percent (57 percent in Singapore) believed destruction to be cheaper than other data sanitization approaches—which simply isn't true.

Figure 10.

Man hours spent destroying devices per month (Base 319)



The average cost reported by respondents to destroy an item is USD $1,036. This means that each company spends just over USD $1.7 million per year in destroying devices. This doesn't include the cost of the item itself—when included, this brings the annual cost to just under USD $4 million per company.

There are also large costs associated with end-of-life devices that are not destroyed, but stockpiled. Our report, *The High Cost of Cluttered Data Centers*, revealed that these cost some enterprise organizations hundreds of thousands of dollars annually for noncompliance or onsite storage fees—charges that could be easily mitigated.[3]

There is a big gap between senior leaders' understanding of the situation and reality. They do not fully understand the security and cost implications of physical destruction and end-of-life equipment lying around, and run the risk of data breaches and noncompliance due to the lack of chain of custody controls. Others are looking to use cost-effective options (including destruction) without realizing they are spending a great deal of time and money on these methods—and risking even more if things go wrong.

Figure 11.

Device destruction costs per company

DEVICE TYPE	AVERAGE COST OF DESTRUCTION PER DEVICE	AVERAGE NUMBER OF DEVICES DESTROYED	TOTAL COST OF DESTRUCTION PER ANNUM	AVERAGE DEVICE VALUE	TOTAL VALUE OF DEVICES DESTROYED PER ANNUM
Mobile Devices	$879	435	$382,365	$1,055	$458,925
Laptops / Desktops	$1,039	404	$419,756	$1,271	$513,484
Servers / Data Center Storage	$1,175	339	$398,325	$1,699	$575,961
Loose Drives	$1,072	475	$509,200	$1,117	$530,575
Total / Average	$1,036	1,653 items	$1,712,508	$1,285	$2,124,105

[3] "The High Cost of Cluttered Data Centers." Blancco, 24 January 2019, www.blancco.com/resources/rs-the-high-cost-of-cluttered-data-centers/

Conclusion

Steps to Minimize the Impact of Data Breaches with Data Sanitization

So, what does best practice look like? Our research shows that a large proportion of enterprises need to review their current processes for managing end-of-life equipment. They should strategically adopt best practice approaches to sanitization to minimize the risk of data breaches, while also reducing costs.

Enterprises have a wide range of options available to erase data from an end-of-life device and the selection of the best method is essential. Physical destruction is an often-used approach, but it is expensive, challenging to meet security requirements, and environmentally wasteful since reuse is not possible. For unfunctional devices, physical destruction is the only real option. However, at end-of-life, as well as during the other stages of the device's lifecycle, enterprises should develop policies that integrate data erasure using software-based tools. This provides certified, auditable sanitization while also reducing business risks.

Data sanitization best practices:

- Ensure data sanitization policies are up-to-date and communicated to all employees across the enterprise.
- Minimize delays in dealing with end-of-life equipment to reduce security risks and avoid unnecessary costs.
- If physical destruction is embedded in policy, ensure different processes are followed for SSDs and HDDs, paying particular attention to shred sizes.
- Build integration into asset management solutions to automate process flow, improve efficiency and reduce costs, while also reducing the number of manual steps and the risk of human error.
- Improve the management and awareness of end-of-life devices to avoid stockpiling and reduce internal threats.
- Ensure there is a clear chain of custody for device management, including a certified data erasure process.

Physical destruction is not your only choice for protecting end-of-life data. Read "**Physical Destruction vs. Secure Data Erasure**" now.

About Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

With Blancco Mobile Insurance, Blancco Mobile Buy-back/Trade-in and Blancco Mobile Retail solutions, organizations can achieve real-time valuation for mobile devices with a simple solution that enables consistent, accurate and measurable testing, including market-leading cracked-glass detection.

Additionally, mobile processors can achieve operational excellence while maximizing profits with Blancco Mobile Diagnostics & Erasure—a purpose-built solution that features our industry-leading Blancco Mobile Workflows for key processing insights across the entire mobile device lifecycle.

For more information, visit our website at www.blancco.com.