Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

Disentangling the Myths: Why Data Erasure and Encryption Is Not Data Sanitization

INTRODUCTION

The importance of proper data sanitization in the disposal of end-of-life hardware cannot be overstated. It is crucial to employ effective methods for data disposal to protect sensitive information from falling into the wrong hands.

The most common misinterpretation is interchanging the term data sanitization with data erasure/data encryption.

Mistakenly, data encryption and erasure software have often been confused as data sanitization methods; we will analyze the considerable risks associated with these methods and why they are not considered enterprise-grade data sanitization methods.

This white paper will also explore ITAD as a destruction service and show how on-site physical destruction is the only effective and cost-friendly method to ensure proper data sanitization.

DATA ENCRYPTION

Encryption is an effective method used to enhance data security only during the active operation of a host/server.

For background: This technique involves converting data into a coded form, making it unreadable to unauthorized individuals. By implementing encryption, organizations can ensure that their sensitive information remains confidential and protected from threats.

However, it is important to acknowledge the limitations of encryption regarding hardware as devices reach the end of their lifecycle. They may no longer receive necessary updates and patches, leaving them vulnerable to hacking attempts. This can pose a significant risk to the encrypted data stored on such hardware. It is essential to understand that if a “bad” actor gains unlimited time with an intact drive, the chances of compromising the data are highly likely. 48-bit encryption, considered the gold standard 12 years ago, took 4.5 days of brute force attack to compromise; today’s technology enables hackers to perform the same in 1.5 minutes.

Today’s encryption that is not updated will be compromised by tomorrow’s skillset and technology.

Despite the implementation of encryption, there are still vulnerabilities present that could potentially result in data breaches or unauthorized access. Organizations must remain vigilant and aware of these risks to protect themselves. Necessary precautions must be taken to prevent any potential breaches from occurring. Failure to address these vulnerabilities could have severe consequences for both individuals and businesses. These incidents highlight how even seemingly secure systems can be compromised by skilled hackers or malicious insiders.

In 2018, there was a notable data breach in encryption involving a widely used protocol called WPA2, which is employed to secure Wi-Fi networks. This security vulnerability, known as the KRACK attack (Key Reinstallation Attack), specifically targeted the WPA2 encryption protocol used for Wi-Fi networks. By exploiting a weakness in the WPA2 protocol, attackers could force devices to reuse encryption keys and gain access to sensitive information transmitted over Wi-Fi networks. The impacted devices included computers, smartphones, and IoT devices.

Crypto-shredding is a specific approach within the realm of encryption, where the focus is on making encrypted data irretrievable by deliberately discarding the Media Encryption Key (MEK) associated with it. This is done without actually erasing or overwriting the encrypted data itself, the idea being that without the key, the data becomes unreadable. However, this technique is not foolproof, as the risks that apply to encryption in general still remain. For instance, if a copy of the encryption keys is stored somewhere else and falls into the hands of malicious individuals, the data can still be compromised. Additionally, many organizations have hesitated to adopt crypto-shredding as a practice, partly because regulatory bodies such as NIST (National Institute of Standards and Technology) and GDPR (General Data Protection Regulation) do not explicitly mandate or recommend it.

By examining these real-world scenarios, we can better understand the importance of continuously improving our encryption practices and staying vigilant against evolving threats.

ERASURE “SANITIZATION” SOFTWARE

Many software solutions promise to wipe out hard drives, but there’s a general misunderstanding about how these work and what levels of erasure they can truly achieve. For one, data erasure software can never completely destroy information stored in drives. For this reason, the NIST 800-88 and NSA/CSS policies, referred to by many industries, including financial institutions and the government, clearly call out that software sanitization is NOT an acceptable solution to properly sanitize drives.

The publication states that the effectiveness of software sanitization depends on various factors, including the quality of the software, the type of storage media, and the potential presence of hidden or remapped areas on the device. It advises organizations to consider the level of risk associated with the data stored on the media and choose appropriate sanitization methods accordingly.

In summary, while NIST 800-88 does not outright dismiss software sanitization as an acceptable method, it underscores the need to assess the risks involved and adopt more robust techniques, such as physical destruction, when dealing with highly sensitive information. Organizations, including financial institutions and the government, refer to these guidelines to establish comprehensive media sanitization policies.

When it comes to data sanitization, encryption, and erasure are commonly recognized as reliable techniques for protecting confidential information on storage devices. However, per the guidelines outlined in the NSA/CSS POLICY MANUAL 9-12, it is important to note that neither encryption nor erasure can be classified as sanitization methods.

For background information, software data erasure works as follows: The application writes a stream of zeros, ones, or meaningless alpha-numeric data (pseudorandom) onto all the sectors of a hard drive. These mask each hard drive sector. Many data eradication programs give the user the option to do multiple overwrites.

One of the main issues with software data erasure is that it only works partially on flash-based media like USB flash drives and solid-state drives. The issue is that these devices can still keep remnant data that, although made inaccessible to the technique used for the erasure, can still be retrieved using the individual chips inside the drive. For example, if there are bad sectors, these can be invisible to the host system and the erasing software. Any data stored in them would be recoverable.

Software erasure also depends on the integrity and reliability of the erasure software. If the software has bugs or is not up-to-date, it might not effectively delete the data. Moreover, in some instances, firmware or hardware-embedded data might not be accessible or erasable by the software.

In data center or server room operations, time constraints and operational limitations often prevent comprehensive online data erasure in faulty drive situations. The focus is quickly resolving technical issues to minimize server downtime rather than dedicating resources to ensure data erasure. Consequently, even after repairs or replacements, storage devices may still contain sensitive information, creating a significant security risk if not properly sanitized.

Due to the possibility of data remanence, reliance on software integrity, and SSD limitations, software erasure should never be used as an enterprise-grade method of data sanitization of critical information.

ITAD AS A DESTRUCTION SERVICE

Due to budget issues and to mitigate in-house workload, companies increasingly outsource data sanitization to third parties as part of their decommissioning activity. Unfortunately, relying on third-party solutions can expose the organization to data security risks at multiple touchpoints within the decommissioning process, mainly when the transferred assets still contain critical data. Most companies trust ITAD service companies to properly sanitize their devices, perhaps falsely believing that destruction is occurring. However, it is crucial to keep in mind that the primary motivation for ITAD (IT Asset Disposition) companies to be in business is to refurbish and resell devices in the market to generate profits.

It's common practice for vendors not to destroy the IT assets as promised but sell them – sometimes to malicious players. Many ITAD companies rely on "data encryption" or "data software erasure" to provide their clients with a false sense of security that their data has been "destroyed." However, there are genuine ITAD players in the market that can destroy data-bearing assets on-site properly. Be vigilant and ask ITAD vendors questions, including data sanitization methods, chain of custody tracking, and audit capabilities.

In one instance, journalism students from the University of Vancouver bought seven hard drives at $35 per drive from Agbogbloshie e-waste dealers. Agbogbloshie is a digital graveyard in Ghana, home to discarded electronic devices from the United States and other developed nations. These students found bank statements, social security numbers, credit card numbers, and additional personal information in just seven drives. They also retrieved a highly sensitive $22M US defense contract in a drive with contracts with Homeland Security, NASA, and TSA.

Two MIT graduates bought 158 hard drives from eBay and other sources for less than $1,000. The study found that 117 (74%) of the drives contained old data that could be recovered and read. They found that 49 drives had sensitive information, including medical data, corporate financials, personally identifiable information (PII), and more than 5,000 credit card numbers.

Idaho Power Company discovered that 84 of the 230 drives they had contracted Grant Korth, a salvage vendor, to sanitize had been sold to parties on eBay. Those drives contained sensitive information, such as confidential correspondence, proprietary company information, and employees' data.

Kessler International bought 100 hard drives from eBay for six months. Upon investigation: they found that 40% of the drives contained sensitive information.

The long list shows that many companies trust third-party solutions to do as they promised. Unbeknownst to them: the number of reputable data destruction companies needs to grow as more vendors are driven by profit over security. Some even offer to recycle personal computers for free, only to sell them to cybercriminals. Then there's the human error. For instance, Morgan Stanley was alleged in 2020 to have breached their clients' financial information. That's after their ITAD vendor misplaced several pieces of computer equipment storing PII. The resulting fine from the FTC was $35M.

Consequently, it's hardly surprising that a recent study by ZDNet revealed that 59% of second-hand or refurbished hard drives available on online marketplaces contain data that can be traced back to the previous owner or data center.

THIRD-PARTY PHYSICAL DESTRUCTION PAIN POINTS

Third-party destruction processes may encounter several pain points that organizations should be aware of. These pain points can significantly impact the effectiveness and efficiency of the destruction process and can potentially lead to negative consequences if not addressed appropriately.

1. Data centers allocate significant financial resources to physical security budgets, including intrusio detection systems, access controls, security cameras, and screening processes.
2. Relying on third-party vendors for security can undermine or eliminate crucial safeguards.
3. Inadequate camera coverage and access controls in loading dock areas expose them to adverse weather conditions, increasing the risk.
4. Pre-event processing before shred events involve consolidating, verifying, securing, and sealing media items, introducing additional steps, and potential errors or exploits.
5. Additional security resources are required for third-party shred events, which may strain existing guard forces and budget allocations.
6. Third-party shred events on loading docks can cause delays and impact other teams' capacity and project timelines.
7. Technicians performing shred events on loading docks are exposed to adverse weather conditions, contributing to human errors.
8. If third-party vendors handle the destruction process, tighter oversight and controls are needed for the chain of custody.
9. Deep diving into the operations of a third-party vendor in a missing drive investigation provides limited visibility and reliable evidence, especially if hand scanning is used for verification and changes of custody.

Cyberattacks on third-party vendors are on the rise. Criminals target companies that offer data destruction services to multiple entities, enabling them to collect a large amount of information from a single source. It's important to note that organizations are fully responsible for the data they handle, and third-party mistakes cannot absolve them of liability.

DATA SECURITY LAWS AND REGULATIONS

It is crucial to recognize that regulations and legislation governing data destruction are progressively becoming more stringent. This holds particularly true for organizations responsible for handling:

- Classified information and controlled unclassified information (CUI)
- Personally identifiable information (PII)
- Sensitive but unclassified information (SBU), or
- Information for official use only (FOUO)

For example, the General Data Protection Regulation (GDPR) adopted by the EU Commission in 2018 classifies data sanitization as a data processing technique. It also requires organizations that process personal data for EU residents to follow specific steps before destroying the data or the associated hardware. The GDPR regulations apply to any organization that maintains a robust data redundancy of EU consumer/corporate data irrespective of the geographical location of the backup server.

Would data owners want their data encrypted or physically destroyed when the drive is decommissioned?

According to the GDPR, companies are required to completely erase data on end-of-life devices rather than simply deleting it. Furthermore, they must ensure that end-of-life hardware is rendered completely unusable. This can be achieved by stripping the hardware of its magnetic strips using methods like degaussers, which utilize powerful magnetic fields to destroy stored information. Additionally, physical destruction or the use of drive shredders can effectively render the devices inoperable. By adhering to these guidelines, companies can ensure compliance with GDPR while safeguarding sensitive data.

Besides the European GDPR: many other countries have data destruction laws and standards, too.

United States:

- National Institute of Standards and Technology (NIST) Special Publication 800-88 provides guidelines for media sanitization methods.
- Various industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Payment Card Industry Data Security Standard (PCI DSS) for payment card information, include requirements for data destruction.
- NSA/CSS NSA/CSS Policy Manual 9-12 Storage Device Sanitization and Destruction Manual

Canada:

- Personal Information Protection GDPR Documents Act (PIPEDA) sets out requirements for protecting personal information, including secure data disposal.

Australia:

- Australian Privacy Principles (APPs) specify obligations for organizations to protect personal information, including secure data destruction.

United Kingdom:

- Data Protection Act 2018 incorporates GDPR and includes provisions for secure data disposal.

European Union:

- DIN 66399 (Deutsches Institut für Normung)
- ISO 27001 (International Organization for Standardization)
- DPR (Ireland Data Protection Commission)

These policies provide guidelines for government and private entities on properly handling and protecting personal information through disposal, destruction, or rendering it indecipherable.

Added to that is the Federal Trade Commission, which requires individuals or businesses that use consumer reports for business’ sake to dispose of the resulting data under strict guidelines. Electronic media and files, for instance, must be destroyed or erased in a way that makes consumer data unreadable. On their end, paper records must be burned, shredded, or pulverized.

Specific industry compliance regulations boast their own sets of data destruction instructions, which include rules on data sanitization, data shredding services, and more. These industry laws and regulations have varying restrictions. Some, like HIPAA, which deals with consumer health-related information, limit how long you can store sensitive data on certain operating systems. That means you may need to destroy data regularly. Social media and cloud computing companies with customer health-tracking apps, chat groups, or databases may fall under the HIPAA data governance policy.

Any non-compliance can attract hefty fines. For instance, not adhering to GDPR requirements can risk your organization a fine of $22.6M or 4% of the organization's global turnover, whichever amount is higher. Non-compliance also increases the risk of a data breach, further escalating the financial consequences of compensations and lawsuits. All while putting data owners at risk of fraud and identity theft.

Adding complexity to the situation, data center and server room technicians, by design, lack awareness of the specific types of applications (compute or store) hosted on servers. These applications could encompass a range of sensitive data, such as EU consumer information, corporate financials, application code, or patent architecture. Consequently, treating every device uniformly becomes imperative to mitigate risks and ensure adherence to the most stringent data sanitization standards.

Effectively managing data compliance entails thoroughly understanding various aspects, such as the data's location, extent, sensitivity, and regional governance regarding security. Consequently, ensuring consistent and meticulous sanitization of data devices becomes an exceptionally demanding undertaking.

WHAT DOES A BREACH COST COMPANIES

It took years to quantify the Equifax Inc. breach in 2017 to determine the financial fallout of the data breach it disclosed that potentially compromised the personal information of 143 million consumers.

But researchers who have studied similar incidents say the size and sensitive nature of the information involved in Equifax's breach means it could become one of the most expensive breach recoveries in history.

Data breaches come with immediate expenses like victim notification, investigations, legal fees, fines, and intangible damages such as lost business, reputational harm, and increased insurance premiums, burdening companies for years. According to a report commissioned by International Business Machines Corp and conducted by the Ponemon Institute LLC, data breaches cost U.S. companies an average of $7.35 million in 2017.

U.S. firms pay about $225 per record breach; if you multiply $225 by the 143 million records stolen from Equifax, that's in excess of $32 billion.

Major breaches can far exceed these numbers. For example, Target Corp. disclosed in a May 2017 regulatory filing with the U.S. Securities and Exchange Commission that a 2014 data breach that compromised the names, addresses, and phone numbers of 70 million people has cost the company $292 million so far, with only $90 million of that covered by insurance.

The 12 biggest data breach fines, penalties, and settlements so far:

1. Didi Global: $1.19 billion	7. WhatsApp: $255 million
2. Amazon: $877 million	8. Home Depot: ~$200 million
3. Equifax: (At least) $575 Million	9. Capital One: $190 million
4. Instagram: $403 million	10. Uber: $148 million
5. T-Mobile: $350 million	11. Morgan Stanley: $120 million (total)
6. Meta (Facebook): $277 million	12. Google Ireland: 102 million

These companies have incurred a significant financial loss, amounting to approximately $4.4 billion and steadily rising, due to hacks and data thefts. These incidents have occurred as a result of vulnerabilities or noncompliance in their security systems. Whether it's through attempts to conceal or downplay the breaches or due to preventable errors, these incidents have had detrimental consequences.

DESTROYING DATA SECURELY: ON-SITE DATA DESTRUCTION

After careful evaluation, it has been determined that data encryption and data erasure yield ineffective results in terms of data sanitization. Moreover, ITAD services present numerous risk factors in the secure data handling, and the cost to address breaches runs into millions of dollars. Given these circumstances, on-site asset destruction is the most viable solution for ensuring the thorough sanitization of critical data.

All data, including CUI, PII, FOUO, and SBU, should be destroyed at end-of-life on-site, with adequately rated equipment to maintain utmost security. Organizations must prioritize the secure disposal of data. Established guidelines like DIN 66399 (Deutsches Institut für Normung) furnish valuable instructions to help achieve this objective. Consequently, developing a comprehensive ISO 27001 (International Organization for Standardization), Disposal and Destruction policy becomes essential in conforming to these rigorous standards.

When it comes to on-site data destruction, careful consideration should be given to selecting equipment that meets or exceeds high destruction standards. Shredders or disintegrators are the optimal choices for this purpose. Ensuring the suitability and reliability of the chosen equipment involves checking for requisite certifications such as DIN 66399 compliance or certifications from reputable organizations.

Of equal importance are clear protocols governing collection, segregation, and preparation stages before destroying data – integration of secure containers into these procedures is highly recommended.

Additionally, establishing processes capable of confirming effectiveness in eradicating all traces across distinct media types stands critical.

Throughout the development of such protocol, it is of utmost importance to ensure a completely tamper-proof chain of custody. This entails providing comprehensive documentation that offers detailed insight into every stage of the data disposal process.

In the case of selecting a data destruction solution, one notable product worth considering is the Phiston line of products for end-of-life destruction. These products meet or exceed the highest destruction standards, including DIN 66399 compliance. It can securely destroy a wide range of media types, such as hard drives, solid-state drives, and motherboards.

CONTROL OVER THE DESTRUCTION PROCESS

Sensitive data controlled by the government or private organizations should always be accounted for. That means going beyond keeping it safe to document what your organization has done to safeguard data erasure.

Such measures can quickly become cumbersome when your organization manually tracks decommissioned hard disks. For example, by monitoring their processing before shipment, tracking them during shipment to the vendor’s destruction facility, and confirming they have been wholly obliterated.

On-site data destruction processes can ease the documentation by removing the following:

- Third-party stakeholders.
- Visibility issues associated with relying on an outside partner to destroy a hard drive or delete data.

From a regulatory compliance perspective, gaining control over the data being destroyed is helpful. But it also makes it easier to safeguard against insider threats.

Sure, people in your organization can still access decommissioned IT assets, but you limit that possibility. Instead of being in the dark, not knowing who handled your decommissioned hard disks at what point in time increases the risk of insider threat.

Plus, it’s easy to monitor and safeguard disposable IT assets when dealing with a few. Different from a disposition vendor who is handling 1000s of such daily.

VERIFICATION OF DESTRUCTION

You have multiple options when it comes to destroying data. However, they all function differently.

For instance, physical destruction is only effective if the IT asset is shredded completely. (Any access to substantial parts of the decommissioned hardware can allow malicious players to recover data.) It gets worse in data destruction software data wipes, as those are more vulnerable to leaving recoverable data.

Ensuring a reliable data disposition company partner is crucial for mitigating risks like human error and improper destruction methods. Verify their expertise, sanitization tools, and reputable certifications from government agencies like NAID AAA, NSA/CSS, or GSA Schedule 70.

Then again, keeping the destruction process in-house helps eliminate these shortcomings because you can verify proper deletion at every step.

COST BENEFIT ANALYSIS OF IN-HOUSE PHYSICAL DESTRUCTION

It is a misconception that effective destruction equipment is prohibitively expensive.

A cost-benefit analysis of implementing one of Phiston's All Media Destruction machines proves to be a more budget-friendly option than off-site destruction. The analysis focused on several key factors, including the initial investment required for setting up the necessary infrastructure. Additionally, we will compare the ongoing costs associated with third-party services.

In terms of ROI, on-site destruction makes the most budgetary sense. Our savings calculations assume a moderately sized data center campus must sanitize approximately 12,000 HDDs, 2,000 SSDs, and 500 other media devices conservatively yearly.

Based on these assumptions, a 5-year Cost Benefit Analysis using very conservative numbers considering decommissioning events per year on campus, the return on investment is ONLY 10 months, with a 5-year savings south of $600k per campus.

On a cost-per-unit basis, off-site shredding costs, on average, are $12/drive vs. $3.75/ drive in-house.

Our savings calculations consider all maintenance costs during the 5-year period and the labor required to perform the sanitization. The costs for in-house destruction remain consistent, whereas the expenses associated with off-site disposal services are uncertain and fluctuate monthly, posing challenges for budgeting. Additionally, there seems to be no end in sight to the continued spending. In-house destruction eliminates those variables and enables DC-Ops to accurately forecast year over year by having a fixed cost. (See Appendix A)

CONCLUSION

This paper highlights the limitations of relying solely on encryption and erasure software for data disposal, as they don't provide true data sanitization and can lead to breaches. Concerns also arise with third-party ITAD destruction services, including trust and potential data breaches. To mitigate these risks, organizations should adopt a robust multi-layered approach. In-house physical destruction emerges as a viable solution, offering control, a Certificate of Destruction, and long-term cost savings.

Phiston Technologies offers advanced R&D and customized solutions to protect against data breaches. With tailored guidance, organizations can address their unique security needs. Continuous research and staying updated are crucial, given the evolving data security landscape. Phiston specializes in proactive product development and agile innovation. They excel in secure on-site data destruction, using advanced technologies to safeguard sensitive information.

Partnering with Phiston Technologies gives organizations access to expertise, customized solutions, and proactive product development. Phiston empowers customers to fortify their data security measures effectively, tackling control over their data disposal processes.

REFERENCES

NIST. (2012). NIST Special Publication 800-88 Revision1: Guidelines for Media Sanitization.

NSA/CSS. (2020). NSA/CSS Policy Manual 9-12: Destruction and Disposal of Information Systems Storage Media and Sanitization.

Office machines – Destruction of data carriers – Part 1: Principles and definitions, English translation of DIN 66399-1:2012-10

Office machines – Destruction of data carriers – Part 2: Requirements for equipment for Destruction of data carriers, English translation of DIN 66399-2:2012-10

ISO/IEC 27001(2013) (International Organization for Standardization)

KRACK Attacks: Breaking WPA2. (2018). Retrieved from https://www.krackattacks.com/

Agbogbloshie e-waste and the University of Vancouver case study. (2009). Retrieved from https://www.cbc.ca/news/science/b-c-students-buy-sensitive-u-s-defence-data-for-40-in-africa-1.803353

MIT graduates' study on hard drives purchased from eBay. (2003). Retrieved from https://news.mit.edu/2003/diskdrives

Idaho Power Company and Grant Korth case. (2006). Retrieved from https://www.computerworld.com/article/2555144/idaho-utility-hard-drives----and-data----turn-up-on-ebay.html

Kessler International's investigation on hard drives purchased from eBay. (2009). Retrieved from https://www.computerworld.com/article/2530795/survey--40--of-hard-drives-bought-on-ebay-hold-personal--corporate-data.html

Morgan Stanley's breach incident and FTC fine. (2022). Retrieved from https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html#:~:text=Morgan%20Stanley%3A%20%24120%20million%20(total,relating%20to%20its%20data%20security