INSTITUTE FOR HOMELAND SECURITY

FORENSIC DIGITAL DATA SANITIZATION:

A GUIDE FOR SMALL AND MEDIUM-SIZED BUSINESSES

Institute for Homeland Security

Sam Houston State University

Narasimha Shashidhar

Cihan Varol

Forensic Digital Data Sanitization
A Guide for Small and Medium-Sized Businesses
A Primer on Data Erasure: An Integral Component of Data Lifecyle Management

Authors: Narasimha Shashidhar, and Cihan Varol

Contents

1 Introduction and Overview

Data Sanitization is a catch-all term meant to capture the processes behind permanently destroying digital data on electronic storage media. In principle, the data is expected to be destroyed irreversibly, i.e., one that renders any forensic data recovery process moot and ineffective. Typically, this may at times also include obliteration of the physical storage medium in question, depending on the security measures employed, confidentiality level sought, and the sensitive nature of the stored data under the operating environment. While most large corporations have effective data sanitization systems in place, research has shown that small and medium -sized businesses at times fail to perceive the significance of data sanitization, and worse, are indifferent to it, often at their peril. This has the potential for a business disaster and leads to their downfall and collapse, often times precipitously.

The focus of this white paper is on developing solutions and guidelines to equip a typical SMB proprietor with essential tools and techniques that will permit them to manage their data safely and effectively, including sanitization procedures. Our goal for this project is two-fold as outlined herein: develop a data sanitization plan, and a disaster recovery plan that integrates data erasure principles effectively into the business continuity plan. This is a timely, contemporary, and a highly important issue for SMBs because of the burden of penalties placed on them by law, governmental policies, regulators, and risk assessment frameworks. Our research, therefore, will empower a SMB proprietor with tools and techniques to accomplish data erasure processes that are cost- and time-efficient.

2 How to Use This Whitepaper

Currently, to the best of our knowledge, there exists no major study in the literature that is comprehensive, accessible, and budget-friendly to the average SMB proprietor for implementing data erasure principles with a turn-key solution. Presently, the amount of data generated by organizations, big and small, is immense and growing exponentially. With the growth in IoT, this volume is only bound to increase. Governments, society, and individuals, alike are highly concerned about privacy and confidentiality issues, and not limited only to PII, health data, etc. On the other hand, storage technologies are rapidly increasing in size, and getting cheaper by the day. Our research and subsequently, this whitepaper, is a potential solution to address these issues head-on. We present detailed strategies, accompanied by instructional videos outlining these enumerated goals below:

- Data erasure standards, analysis, and codification.
- Erasure and Sanitization strategies.
- Disaster Recovery Plan.
- Business Continuity and Data Lifecyle Management.
- Asset Management and Data Management Integration plan.

Our goals for this project are to:

1. Outline the importance of data sanitization plans as part of a holistic data lifecycle management plan in a small and medium sized business.
2. Identify standards and operating procedures outlined by NIST, and other governmental and scientific bodies to effectively implement a sound data sanitization plan.
3. Equipping small businesses with appropriate ***strategies and cost- and time-effective*** techniques to:
    1. Sanitize a diverse array of electronic storage media.
    2. Implement best practices for Business recovery and disaster recovery procedures as it relates to data lifecycle management and sanitization.
    3. Minimize a SMB's footprint and consequently the attack surface area for data breaches, and related threats using sound data management techniques.
    4. Integrate IT asset management recycle, upgrade, reuse policies with data sanitization principles.
    5. Ensure business compliance with regulatory bodies by building forensically sound verification of sanitization processes.
4. ***Disaster Recovery and Data Lifecycle Management Principles***
    1. Creation of security policies and appropriate awareness training for data management.
    2. Standards, practices, and legislation to ensure compliance by the SMB.
    3. Principles of minimizing data footprint and threat/attack surface area.
    4. NIST, ISO, and DoD principles governing data erasure, sanitization, and lifecycle management.
    5. Ready to use, turn-key, disaster recovery plans with integrated data erasure/sanitization procedures.
5. ***A SMB friendly video walkthrough of data erasure techniques***

2.1 Economic Loss

Data attacks and breaches cost businesses in the U.S. untold sums of damage. Failure to comply with security policies, and regulations, both at home and abroad such as GDPR, CCPA, and others lead to fines, and consequences that are devastating to companies of all sizes. Under Article 17 of the UK GDPR[i], individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. In an effort to satisfy these myriad policies, and data principles, companies have adopted data sanitization and erasure as a part of their data lifecycle management plan. This is also propitious since it minimizes companies' footprint and exposure to threat actors. This is particularly true for SMBs since a mistake of any proportion in data management can lead to dissolution, or insolvency for the SMB.

3 Importance of Data Sanitization

We contend that with the increased generation of data, interconnectivity of devices, and cheaper storage, systematic, and effective data management lifecycle procedures that incorporate data erasure and sanitization mechanisms are imperative in today's business environment. This need is further exacerbated in the SMB framework, because these business environments are not adequately equipped to handle the challenges inherent in data sanitization. This is all the more stressful since many of these businesses are operating under pressure of law, policy, or regulation

to maintain and dispose of data in a prescribed manner. A common but often overlooked issue is in IT asset management. In particular, in an effort to be environmentally responsible several businesses prefer recycling, and repurposing computing devices. This is commendable since destruction of electronic waste is harmful to the environment. However, absent sound erasure techniques, data leakage is inevitable and may lead to losses of greater magnitude in terms of fines, penalties, and damage to business reputation. To this end, sound data sanitization techniques are relevant in many distinct applications and several different small- and medium-sized business arenas to minimize downtime and lost profits and revenue.

3.1 Integration into Holistic Data Lifecycle Management Plan

Data lifecycle management typically encompasses the techniques surrounding the data, from inception to destruction. The life cycle of a digital '*bit*' looks something like this: a. Creation,

b. Secure storage,
c. Authorized usage, and
d. Ultimately erasure or secure destruction.

The lifecycle stages are self-explanatory and make inherent sense. Once data has been generated by a business process, this data item needs to be stored securely, used in an authorized fashion, and eventually destroyed in a secure manner. These stages are intended to maximally manifest the principles of the CIA Information Assurance triad[ii], namely confidentiality, integrity, and availability. Clearly, confidentiality (or more colloquially, privacy) of customers' data is paramount to a SMB. The integrity of the information stored and finally availability of the stored data directly impacts the bottom line of a business. It is primarily in the erase/destruction phase of the data lifecycle management do we find ourselves confronting the sanitization challenges.

4 Some Standards and Operating Procedures

NIST, ISO, and DoD (Department of Defense) have established principles and guidelines governing data erasure, sanitization, and data lifecycle management. We will talk about these standards in Section 6.3. In the next subsection, let us look at some effective techniques for implementing a sound data sanitization plan.

4.1 Effective Implementation of a Sound Data Sanitization Plan

Most discussions on implementation of a sound data sanitization plan begin with a reference to the seminal work done by the organization called Sustainable Electronics Recycling International, SERI. In particular, their ANSI approved R2v3[iii] standard (R2 stands for reuse and recycling) exemplifies the best practices and standards in data erasure. Appendix B of the standard is relegated to implementing effective data sanitization techniques and strategies. Table 1 of the report outlines strategies for physical destruction of storage media and the *Logical Sanitization* portion of the report's appendix outlines erasure techniques. A straightforward turnkey approach to implementing such an R2v3 data sanitization plan is outlined in their knowledge base[iv]. Rather than duplicate the contents of the report in this whitepaper, we recommend the interested reader to peruse the original report.

5 Equipping Small Businesses with Appropriate Strategies

5.1 Diverse Electronic Media

Relying on a single electronic media platform or medium can be risky. Technical failures, cyberattacks, natural disasters, or other unforeseen events can render a particular platform inaccessible or compromised. By diversifying media options, businesses can mitigate the risks associated with such events and minimize the impact on their operations. Diverse electronic media ensure that a business has redundant systems and backup options in case of failures or disruptions. If one medium or platform fails or experiences issues, alternative media can be relied upon to ensure the continuity of operations. This reduces the risk of data loss, downtime, and service disruptions. Overall, by embracing various media platforms, businesses can safeguard their operations, enhance their market presence, and maintain a competitive edge.

5.2 Integration into Business Recovery and Disaster Management Plans

By integrating data sanitization into the disaster recovery and business continuity plans, one can minimize the risk of unauthorized access or misuse of sensitive data during a disaster. It helps protect the organization's reputation, maintain regulatory compliance, and mitigate potential legal and financial consequences. In other words, integrating data sanitization into disaster recovery plans is crucial to ensure the security and privacy of sensitive information during and after a disaster. Determining which data needs to be sanitized based on its sensitivity, legal requirements, and relevance is crucial. Classifying data into categories such as highly sensitive, moderately sensitive, and non-sensitive to establish the priority for sanitization during the recovery process is an important step. The data sanitization needs to take place before data backup, during restoration, and after recovery in three consecutive steps. The entity needs to evaluate the necessary resources, timeframes, and personnel responsible for executing the sanitization activities.

5.3 Minimize Digital Footprint and Attack Vector Surface Area

Data sanitization plays a critical role in minimizing digital footprints and reducing the attack vector surface area. Data sanitization ensures that sensitive information is permanently removed from storage devices, making it inaccessible to unauthorized individuals. Simply deleting files or formatting storage devices may leave behind residual data that can be recovered using specialized tools. Data sanitization techniques, such as data wiping or secure erasure methods, overwrite the storage media with random or predefined patterns, making it extremely challenging or impossible to recover any meaningful data. Data sanitization helps prevent unintentional data leakage. When disposing of storage devices or transferring them to other parties, such as through recycling or reselling, it's essential to sanitize the data first. Data sanitization is also vital in mitigating insider threats. Employees or individuals with authorized access to data can pose a risk if they intentionally or inadvertently misuse or leak sensitive information. By regularly sanitizing data and removing unnecessary or outdated files, the potential attack surface from insiders is minimized. It also eliminates unnecessary or redundant information, reducing the potential targets for attackers. Data sanitization helps meet General Data Protection Regulation (GDPR) and the California Consumer

Privacy Act (CCPA) compliance requirements by ensuring that personal information is permanently removed from storage devices.

5.4 Integrate IT Asset Management Recycle, Upgrade, Reuse policies with Data Sanitization Principles

Integrating IT asset management policies with data sanitization principles is essential for effective data protection, efficient asset management, compliance with regulations, cost savings, environmental sustainability, and building a positive reputation. By combining these principles, organizations can minimize the risks associated with technology assets, protect sensitive information, and demonstrate responsible stewardship of resources.

5.5 Business Compliance with Regulatory Bodies

Compliance with regulatory bodies is crucial for small to medium sized businesses to ensure the protection of sensitive data and maintain legal and ethical standards. When it comes to data sanitization, several regulatory bodies have specific requirements and guidelines that need to be followed.

A. GDRP: Under the GDPR, organizations must implement appropriate technical and organizational measures, including data sanitization, to protect personal data from unauthorized access, loss, or disclosure. When disposing of personal data, businesses must ensure that it is irreversibly anonymized, pseudonymized, or securely deleted.
B. National Institute of Standards and Technology (NIST): NIST Special Publication 800-88 outlines standards for media sanitization, including methods for secure erasure or destruction of data to prevent unauthorized recovery. NIST guidelines emphasize the importance of selecting appropriate sanitization methods based on the media type and sensitivity of the data.
C. Health Insurance Portability and Accountability Act (HIPAA): While HIPAA does not specifically mention data sanitization, covered entities and business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI.
D. Payment Card Industry Data Security Standard (PCI DSS): PCI DSS requires organizations to protect cardholder data and securely dispose of it when it is no longer needed. Data sanitization techniques such as secure wiping or physical destruction of storage media should be employed to ensure cardholder data cannot be recovered.
E. Federal Information Security Management Act (FISMA): FISMA requires agencies to develop and implement policies and procedures for sanitizing media and sanitizing information system components before disposal or reuse.

6 Disaster Recovery and Data Lifecycle Management Principles

6.1 Creation of Security Policies and Appropriate Awareness Training

Creating security policies and providing appropriate awareness training for data sanitization are crucial steps in protecting sensitive information and ensuring data privacy. The following draws a path to fulfill these requirements.

Developing Security Policies:

Creating comprehensive security policies is essential for organizations to establish clear guidelines and standards regarding data sanitization. Here are some key steps to consider:

A. Identify Data Categories: Data needs to be categorized based on its sensitivity level, such as personally identifiable information (PII), financial data, intellectual property, or trade secrets. This classification helps determine appropriate sanitization methods for different data types.
B. Assess Legal and Regulatory Requirements: Legal and regulatory obligations that apply to the organization need to be understood (covered in Section 5.5). The security policies should be aligned with these requirements.
C. Define Data Retention and Disposal Procedures: Guidelines needs to be established on how long data should be retained based on legal requirements and business needs. Secure data disposal methods should be developed, including secure erasure or destruction techniques, and need to specify who is responsible for executing them.
D. Implement Access Controls: Roles and permissions need to be defined for employees to access and handle sensitive data. Access needs to be limited to authorized personnel only and should implement strong authentication measures, such as multi-factor authentication (MFA), to prevent unauthorized access.
E. Monitor and Audit: Establishing a real-time monitoring mechanism to track data handling activities, including data sanitization processes are vital. Regular audit and review of security measures are needed to identify any vulnerabilities or areas for improvement.
F. Incident Response: Developing procedures to address data breaches or incidents involving data exposure is crucial. Outlining the steps to be taken in the event of a breach, including reporting, containment, investigation, and recovery is needed.

Appropriate Awareness Training:

Alongside security policies, organizations must provide awareness training to employees to ensure they understand the importance of data sanitization and their role in safeguarding sensitive information. An effective awareness training should include:

A. Training Objectives: Training objectives need to be defined, which may include educating employees about the types of sensitive data, the risks associated with mishandling it, and the importance of proper data sanitization practices.
B. Tailored Training Modules: Training modules need to be developed that are specific to different employee roles and responsibilities. For example, IT personnel may require indepth technical training on data sanitization methods, while non-technical staff may benefit from general awareness training on data protection best practices.
C. Engaging Content: Using a variety of training methods such as presentations, videos, case studies, and interactive quizzes to make the training engaging and memorable is an effective method. Real-life examples and scenarios can help employees understand the impact of data breaches and the importance of data sanitization.

D. Reinforcement and Updates: Providing regular refresher courses to reinforce key concepts and addressing any updates to security policies or regulations are vital. Employees need to be informed about evolving threats and emerging data sanitization techniques.
E. Communication Channels: Establishing effective communication channels for employees to report potential security concerns or seek clarification on data handling practices are needed. Encouraging a culture of open communication and emphasizing the importance of reporting incidents promptly will create a more secured environment.
F. Ongoing Evaluation: Continuous assessing the effectiveness of the awareness training program through feedback surveys, quizzes, and performance evaluations need to be utilized.

Overall, data sanitization is an ongoing process, and security policies and awareness training should be regularly reviewed and updated to keep pace with evolving threats and regulatory changes.

6.2 Standards, Practices, and Legislation to Ensure Compliance by the SMB

Small-to-medium-sized businesses (SMBs) need to comply with various standards, practices, and legislation to ensure proper data sanitization and maintain regulatory compliance. Section 5.5 covered the regulations/standards that need to be complied with by an SMB in data sanitization process. Depending on the industry in which an SMB operates, there may be specific regulations or standards that apply to data sanitization. For example, SMBs in the financial sector may need to adhere to regulations such as the Gramm-Leach-Bliley Act (GLBA) or the Sarbanes-Oxley Act (SOX), which have data sanitization requirements. In addition to these standards and legislation, SMBs should also consider best practices recommended by cybersecurity organizations and industry associations. Staying informed about emerging regulations and industry-specific guidelines is crucial to ensuring ongoing compliance with data sanitization requirements. Collaborating with cybersecurity professionals and seeking legal advice can also help SMBs navigate the complexities of compliance in data sanitization.

6.3 NIST, ISO, and DoD Principles Governing Data Erasure, Sanitization, and Data Lifecycle Management

NIST, ISO, and DoD (Department of Defense) have established principles and guidelines governing data erasure, sanitization, and data lifecycle management.
NIST Special Publication 800-88: "Guidelines for Media Sanitization", outlines recommended practices for securely sanitizing media, including storage devices and other physical media. It defines different sanitization methods, such as overwrite, cryptographic erase, degaussing, and physical destruction.

ISO/IEC 27001: "Information Security Management Systems (ISMS) - Requirements": This standard provides a framework for establishing, implementing, maintaining, and continually improving an information security management system. It includes requirements for secure data erasure and sanitization as part of the overall data management process.

ISO/IEC 27040: "Information technology - Security techniques - Storage security": This standard focuses on the secure storage and management of information, including data sanitization. It provides guidance on secure data erasure methods, media disposal, and overall data lifecycle management.

DoD 5220.22-M: "National Industrial Security Program Operating Manual (NISPOM)": This manual provides guidelines for the protection of classified information. It includes requirements for the sanitization of classified media, specifying methods such as overwriting, degaussing, or physical destruction.

DoD 5200.01: "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)": This directive establishes policies and procedures for the protection of sensitive and classified information. It includes requirements for secure data erasure and sanitization to ensure the protection of sensitive data throughout its lifecycle.

These principles and guidelines from NIST, ISO, and DoD form a foundation for secure data erasure, sanitization, and data lifecycle management. Organizations can refer to these standards to develop their data management practices, implement appropriate data sanitization methods, and ensure compliance with regulatory requirements. It is important to regularly review these standards and adapt practices as new guidance or updates are released.

6.4 Ready to use, Turn-key, Disaster Recovery Plans with Data Erasure

Ready to use Disaster Recovery Plan with Data Erasure function follows a comprehensive framework to ensure effective recovery and secure data erasure. Specifically, the cloud-based disaster recovery plan with data erasure function aims to ensure the restoration of systems in the cloud while maintaining secure data erasure during the recovery process. By conducting a thorough risk assessment and business impact analysis, potential risks and their impacts on cloud- based systems and data need to be identified and prioritized. Roles and responsibilities are defined for the cloud disaster recovery team, including those responsible for data erasure. The plan should include backup and recovery procedures tailored for cloud environments, with a focus on maintaining data integrity. Communication protocols needs to be established to notify stakeholders, while regular testing and maintenance activities should be in place to ensure plan effectiveness. Data erasure procedures specific to the cloud environment need to be outlined, adhering to recommended methods and compliance standards. Detailed documentation and reporting capture recovery efforts and data erasure activities are part of the process. Training and awareness programs equip the team with the necessary knowledge to carry out their roles effectively in disaster recovery efforts. Regular reviews and updates will ensure alignment with changing cloud infrastructure, emerging threats, and regulatory requirements, integrating the plan into the overall business continuity strategy.

7 Conclusion

In this research, we discussed strategies and put forth a primer that will serve as a simple guide for proprietors of small- and medium-sized businesses in implementing their data erasure and

sanitization policies and procedures. We hope we have instilled the importance of this monumental task and identified the perils of abandoning this critical task. We've talked about ITAD (IT Asset Management and Disposition), NIST, SERI, and EPA guidelines. We've pulled together and amalgamated a lot of valuable resources into a wholistic document aimed to elide jargon and distill the most essential aspects of the data management lifecycle principles. We truly hope that this primer and the accompanying video are helpful to the SMB owner. We'd also like to take this opportunity to thank the Institute for Homeland Security, The Department of Computer Science, and Sam Houston State University, for their support.

8 Acknowledgement

The authors would like to thank the Homeland Security Institute, and The Department of Computer Science at Sam Houston State University, for funding and support in developing this whitepaper.

9 Endnotes

[i] https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf [ii] https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html [iii] https://sustainableelectronics.org/welcome-to-r2v3/ [iv] https://sustainableelectronics.org/knowledge-base/guidance-for-developing-an-r2v3-data-sanitization-plan- version-1/

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Shashidhar, N. & Varol, C. (2023) Forensic Digital Data Sanitization A Guide for Small and Medium-Sized Businesses A Primer on Data Erasure: An Integral Component of Data Lifecycle Management. (Report No. IHS/CR-2023-1028). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/MF6HJ