Security Issues with Decommissioning Magnetic Media

I. Abstract

This document describes practical considerations of taking magnetic media out of useful service or transferring such media to other departments or organizations. After raising awareness of the security, business, and legal concerns, the document evaluates different techniques for the reader to be able to assess his options. Finally, the cyberCide ™ product is presented as a cost-effective solution to address these risks.

II. Executive Summary

Over the last several decades, computer information systems have rapidly replaced paper filing systems as the primary storage mechanism for a corporation's organizational memory. Initially the mechanisms already in place for information privacy and security were generally adequate for the new systems since physical access to the media was still necessary to breach confidentiality. However, the advent of computer networks and general mobility of electronic data create entirely new security and privacy concerns.

Awareness of the need for information privacy and security tools and procedures has greatly increased thanks to the ubiquity of the Internet. This awareness has brought about an entirely new industry to address these concerns and "plug the holes" that distributed access creates. Billions of dollars and many of the best minds in the industry go into making access to online data both available to users, and safe from the prying eyes of those who seek surreptitious access to those secrets.

After this enormous investment is made and systems undergo their inevitable upgrades, old computers along with their hard drives and other magnetic storage media are replaced and shipped out the back door – *along with all that data you just spent so much time and money securing…* **It happens every day.**

1. Are you giving away secrets with that old computer?

Compared to the risk of security breaches by foreign "hackers" and viruses propagated over the Internet, it is a lesser known fact that simply deleting files or even reformatting a hard drive does not actually remove the data contained in that file or disk. Therefore the

innocuous act of decommissioning an old computer and transferring it elsewhere is quite probably the most common security and privacy breach ongoing today.

While laws are in place and electronic defenses exist in abundance to make online infractions both dangerous and difficult for the propagator who attempts to breach these safeguards; acquiring data from a decommissioned hard drive not only allows the perpetrator to breach these defenses without there being any indication that an infraction has occurred, but also, depending on the circumstances, may not even be illegal! In some cases, however, the person or organization responsible for allowing this private data out may very well be liable criminally and/or civilly.

2. Liabilities of Insecure Disposal

i. Legal

Persons and organizations in the governmental, legal, financial, and medical communities often fall within the jurisdiction of many federal and state laws that presently exist. In the United States, commonly applicable statutes include the Privacy Act of 1974, the Computer Security Act of 1987, the Gramm-Leach-Bliley Act of 1999 (GLB), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). At the time of this document's writing, several bills are under consideration that may further impact the legal ramifications of data privacy and security, HR1259 Computer Security Enhancement Act, HR2435 Cyber Security Information Act, and HR583 Commission for the Comprehensive Study of Privacy Protection. Certainly there are more to follow.

Existing laws provide for significant civil and criminal penalties for breaches of information privacy within certain industries, especially the medical field (HIPAA) and financial industry (GLB). Future laws can only be expected to increase the liabilities in this regard. Outside of the United States of America, the European Union has in place the 1995 Data Privacy Directive which imposes severe restrictions and penalties for breaches of customer confidentiality. To even be able to do business with an EU organization, non-EU companies must often ensure conformity with this directive and provide contractual guarantees of such compliance.

ii. National Security

Information privacy has always been a primary concern with those tasked with enforcing our national security. Federal law and code are full of statutes mandating the protection of the integrity of both classified and non-classified but sensitive information assets. While guidelines are in place for dealing with the decommissioning of magnetic media, often the recommendations are not followed or the mechanism proposed is no longer effective because of the advancement of technology.

iii. Financial

Breaches in data privacy have catastrophic consequences in financial dealings. Obvious examples such as credit card exposure are so numerous that they no longer warrant media coverage. Industrial espionage from competitors causes huge losses and even destabilizes

economies. Despite these risks, few financial organizations have policies and tools in place to secure or irretrievably eliminate their information assets on decommissioned systems.

iv. Privacy and Trust

Employees and customers are often required to reveal personal information to businesses and organizations which they deal with in the normal conduct of their relationships. Breaches of security involving that kind of data inevitably result in breaches of trust which ruin goodwill and damage the integrity of the responsible organization. Such losses are incredibly difficult to repair.

v. Intellectual Property

Technology companies spend billions of dollars annually to advance their position in industry. Most often, this critical investment in intellectual property loses its competitive value when former employees walk out the door to work for a competitor. If they can leave with an improperly decommissioned piece of magnetic media then its only that much easier.

3. The cyberCide ® Option

cyberCide ™ is a specialized utility that is used to securely erase all data from the storage media in a manner that cannot be undone. Operating from a single, bootable floppy, IT technical staff can start the process of secure decommissioning with just a few simple keystrokes. There are no hardware dongles or other complex components to interfere with the user or otherwise impede rapid operation. CyberCide ® is a low cost solution both in terms of acquisition expenditures and user time, providing a return on investment (ROI) unequaled by other methods. Decommissioning systems has never been easier or more effective than with cyberCide ®

III. Why Decommission Your Systems?

"Moore's Law" states that the number of transistors per inch of silicon doubles every eighteen months. Give it another six months to be deployed to the general industry and the effect is that computers undergo a doubling of performance every twenty-four months. This prediction has held true for several decades and shows no sign of letting up.

Rapid obsolescence of technology is a well established phenomenon. Generally a computer system can not be reasonably supported past one generation behind the present state-of-the-art which means its ROI occurs within four years of its initial deployment then it is no longer cost effective to keep the system online.

The bottom line is that IT organizations anticipate replacing 25% of their computers every year. Decommissioning can take many forms:

1. Redeployment

Decommissioning often just means taking a computer initially designated for one task and reconfiguring it for another, generally less performance intensive task. Its more likely to be cheaper to replace that application server purchased eighteen months ago than to upgrade it, but a clean system install would probably turn it into a great workstation or low-end

system elsewhere in the organization. However, such an install doesn't actually "clean" the old data off the magnetic media so extra care must be taken to ensure that the sensitive information that was stored during its previous life doesn't accidentally show up where it doesn't belong.

2. Donation or Auction

Even when a system no longer has a useful purpose within the organization, there are plenty of other outside establishments that may be able to take advantage of the computer or its components. Low-cost employee purchase plans are popular as are donating the systems to a charitable organization or school. For organizations which have higher-than-normal performance requirements, decommissioned systems may still be considered mainstream in the outside world and could warrant resale or auctioning to recoup some of the investment in bleeding edge technology. As with redeployment, special precautions must be taken to ensure that sensitive data on that computer system doesn't show up where it doesn't belong.

3. Destruction and Recycling

Sometimes old computers are barely worth the effort to truck to the junkyard or, perhaps, they contain information that is too sensitive to risk any possibility of its dissemination outside of the organization. In these cases, it must be understood that junking the computer does not junk its data and while recycling is often an enlightened technique for hardware, it is exactly the opposite of what you intend for your data. Magnetic data is remarkably resilient and most physical disposal techniques in use have little or no effect on the media itself although it may no longer be accessible through conventional means. Before final tear down of the system, extra care must be exercised to keep that data from reappearing elsewhere.

IV. What Does that Old Computer Have on It?

As transistor density increases, so has the storage capacity of magnetic media. The sheer quantity of data existing on computer drives makes it unlikely that all data can even be accounted for by its owners. What's more, the storage space is so immense, odds are that most deleted information hasn't even been overwritten. So what data should IT staff be concerned about?

1. Data You Know You Need Secure

The most obvious consideration is for that data which the system has been deployed to maintain. Accounting, financial, personal, medical, engineering, and other sensitive information owned by the applications running on the system are known liabilities which must be addressed. The vast majority of IT applications are designed to store, access, and protect this information – not to securely erase it from permanent storage. The challenge is how to ensure that this data is irretrievable before releasing its storage media.

2. Data You Didn't Even Know You Had

Besides the data controlled by the system's applications, computers also store significant quantities of sensitive information that aren't necessarily known by their operators. Many applications and even operating systems store passwords, user information, encryption keys, and other sensitive data in various places including configuration files, registry entries, and temporary files. Virtual memory systems write out random contents of application memory to disk in a haphazard manner that makes it impossible to know exactly what is stored on the media. The challenge here is even identifying what information exists before one can go about securing it from undesired retrieval.

V. Legal Ramifications of Information Privacy

Many organizations fall under the jurisdiction of various federal, state, and international laws that provide for protection of certain types of data. These organizations are responsible for securing and preventing the misuse of this data at the risk of both civil and, sometimes, criminal liabilities. While the following information cannot be considered as legal advice, it is a good general overview of the type of considerations certain organizations should bear in mind when decommissioning information systems.

1. Government Agencies

Government agencies are covered by vast numbers of laws, official codes, and standards which spell out what type of data is covered and how this data must be protected from unauthorized access. While its likely that each agency has its own set of standards and procedures, they all generally fall under the confines of laws such as the Privacy Act of 1974 and the Computer Security Act of 1987. Several standards exist that contain recommendations specific to decommissioning information systems.

The National Institute of Standards and Technology (NIST) document SP 800-14, *"Generally Accepted Principles and Practices for Securing Information Technology Systems"* (September 1996) has a section (3.4.6) that deals specifically with the disposal phase of an IT system's life cycle. It states:

> **3.4.6 Disposal Phase**
> The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. The following items should be considered during this phase:
> **Information.** *Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their agency office responsible for retaining and archiving federal records.*
> **Media Sanitization.** *The removal of information from a storage medium (such as a hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.*

Many other similar documents exist although not all deal with issues specific to decommissioning. They tend to focus, instead, on security during the active life of the information system in question. While these issues are indeed important, it is critical that agencies entrusted with enforcing our Constitutionally protected rights not let sensitive data escape out the backdoor.

2. Financial and Insurance Companies

All financial agencies have fiduciary responsibilities to their clients. These have been especially impacted by passage of the Gramm-Leach-Bliley Act of 1999 (GLB) which purports "To enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers, and for other purposes." Title V – Privacy, of GLB, contains two subtitles A, Disclosure of Nonpublic Personal Information and B, Fraudulent Access to Financial Information, which specify protected data, penalties for its misuse, and procedures to be followed to help ensure such protection. Section 500 of GLB starts with the following admonition:

> **(a) PRIVACY OBLIGATION POLICY**.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information.
> **(b) FINANCIAL INSTITUTIONS SAFEGUARDS**.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Subsection (b) clearly places the burden of protection on that of the financial institution and makes it clear that unauthorized access to sensitive information is a clear focus of the United States Congress. Federal code regulations supporting this act are voluminous and, outside of government, further volumes have been written to help covered organizations understand their responsibilities and liabilities under this act. This far reaching act has already had a significant impact on information security. Secure methods for decommissioning magnetic media must certainly be part of any compliant set of procedures.

3. Health Providers and Insurers

Perhaps the only area of data security that has received more attention than the financial industry is that of medical information privacy. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has had a profound impact on the medical community. It defines a new standard for communication between health care providers and payers as well as new protections for patient medical and identifying information. Purporting to be a simplification act, this promised benefit remains unrealized as Congress and responsible federal agencies struggle to codify how this act will be implemented. Much

of this effort is documented in the Federal Register which provides many details on how agencies responsible for implementing this act perceive these issues. Federal Register Vol 65 Number 250 makes the following observations justifying HIPAA's protections:

> (p.82467)
>
> Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:
>
> A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
>
> A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).
>
> An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).
>
> The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).
>
> A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).
>
> ***A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).***
>
> A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).
>
> In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).
>
> A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).
>
> No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

And later

> (p. 82468)
>
> Breaches of Health Privacy Harm More Than Our Health Status
>
> A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

> A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the National Law Journal, May 30, 1994.
>
> A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See Estate of Behringer v. Medical Center at Princeton, 249 N.J. Super. 597.
>
> A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See New York Times, October 10, 1992, Section 1**,** page 25.
>
> A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998) Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. ``Who's reading your Medical Records,''
> Consumer Reports, October 1994, at 628, paraphrasing Sweeny, Latanya, ``Weaving Technology and Policy Together to Maintain Confidentiality,'' The Journal Of Law Medicine and Ethics (Summer & Fall 1997) Vol. 25, Numbers 2,3.

Having detailed the privacy concerns of HIPAA, the Federal Register later defines what data is covered under the act:

> (p. 82496)
>
> Protected Health Information
>
> We proposed to define ``protected health information'' to mean individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form. For purposes of this definition, we proposed to define ``electronically transmitted'' as including information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and ``faxback'' systems. We proposed that this definition not include ``paper-to-paper'' faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail.

The Federal Register then attempts to establish an idea of what kind of safeguards are anticipated without prescribing a specific mechanism for implementing such safeguards:

> (p. 82562)
>
> We do not prescribe the particular measures that covered entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. (That is, as with other provisions of this rule, this requirement is ``scalable.'') Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring that doors to medical records departments (or to file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or passcode. We intend this to be a common sense, scalable, standard. We do not require covered entities to guarantee the safety of protected health information against all assaults. Theft of protected health information may or may not signal a violation of this rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft. Organizations such as the Association for Testing and Materials (ASTM) and the American Health Information

> Management Association (AHIMA) have developed a body of recommended practices for handling of protected health information that covered entities may find useful.
>
> We note that the proposed HIPAA Security Standards would require covered entities to safeguard the privacy and integrity of health information. For electronic information, compliance with both regulations will be required.

The practical result of this act and the federal code to execute it is that any organization handling patient data for health care or insurance purposes must ensure that this data not be disseminated outside of its intended recipients and that mechanisms for securely decommissioning magnetic media that contain such data must be in place.

VI. Current Disposal Techniques and their Costs/Risks

As information technology evolves, so must the methods used to decommission it in a secure manner.

1. Data Storage on Magnetic Media

Magnetic media is still the most common storage mechanism for persistent information in computer information systems. Its storage densities increase exponentially as does its performance to cost benefit. During this evolution many techniques have been used in decommissioning such media:

2. Data Erasure Techniques

i. Deletion via Operating System

Writing data to magnetic media is still generally the most expensive operation that most computer systems perform from a hardware performance perspective. As a result, most operating systems attempt to optimize this aspect of functionality as much as possible. Deleting pieces of information under the control of the operating system (usually as files) does not actually delete the content, rather it simply marks the record or file as deleted in its index or lookup table. While this considerably reduces the write time for the deletion operation, it still leaves the content available for retrieval from the media until such time as it is overwritten with other data. Also, data to be eliminated must first be identifiable by the user so that it may be targeted for deletion in the first place, not always an easy task. This clearly does not alleviate any potential liabilities for the owner yet it is probably the most common way in which data is "erased" from computer systems today.

ii. Formatting of Media

Formatting is the process of making a physical drive available to be used by the operating system of the host computer. It's a "lower level" operation than simple file deletion. This generally consists of writing data to select parts of the drive to create space for directory indices and other house keeping data that the operating system uses to access the media. While there are some types of formatting, often called low-level formatting, that actually write data on the entire drive, the increased size of hard drives has made this a rare exception and not generally available to most users. Formatting a drive does not actually

overwrite your data, it simply "forgets" that it was there. Still, recovery of data from a formatted drive is only slightly more difficult than recovering data from an operating system delete as described above. Many "security-aware" organizations use this technique to clear data from their magnetic media but it is only slightly more effective than deletion via operating system.

iii. Re-Partitioning of Media

Partitioning a drive is simply the division of a physical hard disk into one or more logical drives that may be accessed by the operating system (after formatting as described above). While this is an even lower level operation than formatting a drive, it actually doesn't touch any part of the data beyond the first 512 bytes of the drive itself. Despite the perception of completely eliminating the previously existing logical drive, all the data on that drive is still intact and recoverable. This technique is completely ineffective for secure deletion.

iv. Degaussing

Degaussing is the technique of exposing storage media to extremely powerful magnetic fields for the purpose of scrambling the contents of the media into an unrecognizable mess. For low density media such as floppy drives and tapes, a degaussing tool of adequate power can be a quick and effective way of clearing data. For high-density storage, however, it is more time consuming, less effective, and generally has other detrimental effects. Most degaussing machines are not powerful enough to penetrate the cover of a hard drive to get to the storage platters inside. Therefore the platters must be removed which also ruins the drive. For machines that are powerful enough to penetrate the shielding, the field is so powerful that all the controlling circuitry is also destroyed so the drive is, again, left nonfunctional. While destruction of the drive might be an acceptable consequence, a serious consideration that must be taken into account is the fact that there is no simple way to confirm or verify that the data has truly been eliminated since the drive is no longer useable.

v. Data Wiping

Data wiping is a bit of a misnomer in a physical sense. Data is not actually wiped from the physical media, but is, instead, overwritten with other data. This has the same effect of removing the previous data from the drive and, given certain methods of overwriting, can make it virtually impossible to determine that the previous data ever existed. Data wiping is a very effective method of destroying sensitive information from all magnetic media. For organizations that have large amounts of low-density media such as floppy disks and tape, degaussing might be a more time effective alternative (for that media) but data wiping is clearly superior for high-density media such as hard drives. Data wiping has the additional benefit of leaving the media intact and usable which, therefore, makes confirmation of the operation's success very simple unlike degaussing. Data wiping can also provide flexible tradeoffs between speed and level of security so that a slower but more secure method may be selected that exponentially reduces the theoretical likelihood of any hope for recovery or detection. cyberCide ™ is the most capable data wiping tool that we know of and takes this concept to an entirely new level.

vi. Physical Destruction

Physical destruction can be accomplished through many techniques – some more effective than others. Degaussing high density hard drives, for example, amounts to a physical

destruction technique that is of questionable effectiveness. However, to afford the ultimate protection beyond what even data wiping can theoretically provide, physical destruction techniques that destroy the molecular composition of the media is the only known option. This involves taking the media and smelting it down so it becomes a chaotic mass. Naturally, this is an expensive operation and likely to only be justifiable in decommissioning systems whose data contain information of life and death consequences. It has the obvious downside of making that media unusable and it is questionable as to whether the technique actually provides any more effective protection than the more advanced data-wiping techniques.

3. Data Recovery Techniques

Having gone over the reasons why secure decommissioning is important and what techniques are available for its execution, what are the mechanisms that we must protect our data from being accessed with? The answer to this question inevitably comes down to the level of sensitivity of the data itself and the time and expense that others might be willing to expend to gain access to it.

i. Undelete

For the simple fact that deletion via operating system is the most common way organizations protect their data, undelete tools are the most common methods for recovering that data. If the data area of previously deleted files has not been randomly overwritten by another file (a more unlikely occurrence the larger the drive) then there are dozens of tools, both free and commercial, that make the full recovery of that data as simple as a few mouse clicks or keystrokes. Indeed most of these tools claim their intended use is to restore data that the user erased unintentionally. From a data privacy perspective, the road to serious security breaches is paved with the best intentions. More advanced tools make the recovery of even partially remaining deleted data almost as simple so dependence on operating system deletion is inadequate in all respects.

ii. Unformat

Unformatting is a more advanced technique that takes on two different methods. The most common is simply restoring the previously existing formatting of a newly reformatted system. Some operating systems actually store a backup copy of its directory index that can be restored by a low level utility written for this purpose. Another method is for a utility that walks through all the data on the drive and attempts to rebuild the format information from scratch. The effectiveness of these techniques depends a great deal on the type of operating system that formatted the drive initially and how the system is used. Generally this technique is followed up with low level reads as described below.

iii. Re-Partitioning

Re-partitioning is the counter measure to the use of re-partitioning for data elimination. While it is a low-level technique, it is also quite simple for those aware of it and the result is often 100% recovery of the previously partitioned drive. Even more ironic is that the same tool is generally used for both the initial and "un-partitioning" so there's not even any new software for the attacker to acquire to accomplish his task.

iv. Low Level Reads

Low level reads are techniques which bypass the operating system view of the data and attempt to retrieve data from the physical media itself. Most existing undelete and unformat utilities incorporate this technique internally to accomplish their tasks. Used outside of the context of the controlling operating system format, low level reads allow the attacker to peruse the physical data content of the drive in a haphazard manner which often reveals information that the system owner wasn't even aware existed on the drive.

v. Forensic Software Recovery

Data recovery detectives have many techniques and utility programs to help in their recovery efforts. They generally consist of all the tools described previously but they also add more advanced applications which help them manage and make sense of their progress. The most often used technique is drive cloning software which allows the attacker to make a mirror image of the drive onto other media. This cloned media can be taken away and accessed as a virtual drive. The attacker can be secure in the knowledge that any mistakes made in the recovery process can be easily undone by restoring the cloned data. If the data is on the original media, a tenacious attacker will most likely be able to recover it.

vi. Magnetic Force Microscopy

All the previous methods of data recovery are known as "soft" recovery techniques. Beyond these are the "hard" recovery techniques. They usually involve physically opening the drive to access its storage media directly with a magnetic probe. This is an analog technique that accesses the media outside of the boundaries and limitations of the digital controller used to read or write the data. As the drive controller operates within certain tolerances, a more sensitive tool that can take many different readings can exploit the imperfections allowed by these tolerances and attempt to recover data previously thought to be erased by the digital controller. This technique is understandably "hit and miss" and, in most cases, prohibitively expensive. To circumvent its effectiveness, an erasure technique must account for how such recovery is possible and address these tolerance limitations in a creative manner.

VII. How cyberCide ® Addresses the Issues

cyberCide® has been architected and implemented with the express purpose of becoming the most cost-effective and secure mechanism available for addressing the issues described in this document.

1. Methodology

cyberCide ® takes into account how data recovery is performed and is capable of effectively defeating every known forensic technique. As it operates outside of the limitations of the host computer's operating system environment, it is not subject to constraints of that environment. By providing flexible methods of secure erasure such as those proposed by the Department of Defense, which defeat all "soft" recovery techniques, and Peter Gutmann's seminal paper "Secure Deletion of Data from Magnetic and Solid-State Memory", which defeats even "hard" recovery techniques, cyberCide ® provides the user with exactly the right tool for whatever level of protection is required.

2. Product Features

Boots From a Single 3.5" Floppy Disk

Just insert the floppy disk and turn on the computer. No difficult or time consuming install process.

Boots From a CD

Please contact your CyberScrub sales representative for more information on this process.

Boots From a Network

Please contact your CyberScrub sales representative for more information on this process.

Intuitive, Friendly User Interface

Clean interface highlights your selections and walks you through the software's operation. Clearly identifies the drives, capacity, format, and manufacturer of each media. In just a few keystrokes your sensitive data is being eliminated.

Host Operating System Independent

No matter how esoteric the operating system or problematic the current system configuration may be, cyberCide ® will give full access to your drives, formatted or otherwise.

Log File Generation

Full and comprehensive log file generation, including options/methods required by the U. S. Department of Defense. The log file will also contain the exact contents of any sector that could not be sanitized. This allows the user to determine if the data that remained on disk to too sensitive to permit the release of the media.

Fast

Efficient programming makes the physical drive performance the sole speed limitation during operation. Hot keys are available to make selection of user options even faster for more knowledgeable users.

Flexible Licensing

Per-use and site licenses are available to address the needs of the individual, corporate and governmental organizations. cyberCide ® will always fit within your data protection plan.

No Hardware Dongles

Every effort has been made to make the process of decommissioning magnetic media simple, convenient and take up as little staff time as

possible. This means not attaching annoying and costly hardware devices that may not be compatible with your hardware before executing your system decommissioning procedures. Once cyberCide ® has started the wipe process on your media, the user may take the cyberCide ® floppy out of the drive and start another system.

3. Unique Capabilities

- ✓ **Unlimited Drive Capacity Support**
  Most tools designed to provide similar functions as cyberCide ® obtain their information about the installed drives through main BIOS or operating system dependent calls. In nearly all these cases, it makes them incapable of full support for the newer large capacity drives. Users will discover that, despite advertising claims of overcoming certain DOS or BIOS limitations, other products generally don't offer full support for the latest drive standards (such as ATA-100). Limited or improper support for these standards can result in a product that may mistakenly report a successful wipe even though it partially clears the media. Things to consider are when the product was last upgraded and what features were provided in that upgrade. If a product existed before the standards for new drives existed it is not likely to be very compliant.
  Unlike other products which use 32 or even 16-bit calls, cyberCide ® uses 64-bit addressing calls to the drive devices. This makes it capable of writing out more bytes of data then presently exists in any drive access standard such as ATAPI. CyberScrub LLC tracks these standards very closely so that when new drive standards are released, cyberCide ® will have an update out to support its decommissioning.

- ✓ **Logical Drive or Partition Addressable**
  cyberCide ® recognizes that different types of decommissioning need more flexibility in order to make it cost effective. cyberCide ® is unique in that it is not only able to access the physical drives in the computer but also their individual partitions or logical drives. CyberCide ® provides maximum flexibility with enhanced ease of use. The user may elect to operate on an entire physical drive, a per-partition basis, or any combination applicable to the system's configuration. Each logical or physically addressed device may also have its own level of secure deletion (or even be ignored) selected for it to provide the best security and performance. When selecting physical drive access, even partition tables are destroyed so an attacker will never be able to determine that the drive was ever formatted in the first place, much less recover any content.

4. Verifiable Accountability

Unlike degaussing or other limited physical destruction techniques, cyberCide ® automatically confirms that all data on selected media have been effectively eliminated. Since the drive is left intact and remains usable, the user may also choose to employ low-level read

or other forensic recovery software to further verify that his data is indeed gone. CyberScrub LLC encourages its users to do whatever is necessary to confirm compliance with their data privacy policies and applicable laws and seeks to help make this as simple and inexpensive a task as possible.

VIII. Conclusion

Decommissioning computer information systems and their magnetic media is a critical part of any data privacy and security process. Most organizations have no such component in their standard process and many are not even aware of the liability that currently exists as a result of this inadequacy. This document is intended to both raise awareness of these issues and provide a cost-effective solution to protect against inherent liabilities. To ensure that your organization or data is not at risk, please contact CyberScrub LLC for product information. If your organization does no have a data privacy or security plan or standard in place, CyberScrub LLC provides consulting services to perform risk assessments and help organizations design and implement such processes to mitigate these factors. When it comes to data privacy protection, a false sense of security can be more dangerous than no security.

CyberScrub LLC provides consulting services to business, industry and government for privacy/security compliance. CyberScrub designs custom software applications as well as pre-configured solutions.

For additional information:

CyberScrub LLC
P. O. Box 3146
Alpharetta, GA 30023

Toll free: 888-350-3436
Voice: 770-951-2080
Email: sales2@cyberscrub.com
Web: www.cyberscrub.com
www.cyberscrub.com/cybercide_