Best Practices in Securing Data from Modification:
Cyber-Attack Risk Reduction Strategy (RRS)

January 1, 2015

GreenTec
11720 Sunrise Valley Drive, Suite LL-02
Reston, VA  20191

www.GreenTec-USA.com
www.GreenTec-Media.com
It is unfortunate that in today’s reality organizations must provide protection against loss or damage to data from outside cyber-attack as well as intentional or accidental insider threats.

Due to the attack on Sony Entertainment, media content companies are taking their data offline to protect it from hackers. While data isolation will protect data from outside hackers, it effectively makes the data useless to those that need safe data access. Taking systems and data offline does not necessarily protect them from insider attacks. A disgruntled employee can wreak havoc on valuable company data or render systems unbootable. An individual may be paid large sums of money to delete files by a market competitor or, in severe cases have their family threatened unless they delete files that would be used as evidence in a murder or drug trial.

The simple method of partitioning your data into two basic categories reduces the amount of data that is at risk in your enterprise. Static Data is data that does not change or changes infrequently, while Dynamic Data is data that changes frequently.

By placing Static Data onto a non-modifiable Read-Only media, the threat from damage, deletion, modification or re-formatting is eliminated. This allows your valuable IT security energies to be focused on locking down access to the remaining Dynamic Data that must be frequently updated.

Workstations, laptops and servers can be hardened by implementing boot sector and disk partition protections thereby preventing damage from cyber-attacks like those experienced by Sony.

This paper discusses considerations, approaches and simple steps that can be taken to quickly implement a Risk Reduction Strategy (RRS) for protection of data before a cyber-attack occurs and a strategy that minimizes damage when a cyber-attack occurs. Capabilities and features of the various Read-Only media available in the market today are also discussed.

Cyber-Attack is Imminent

While no single solution can protect from every possible threat, there are simple easy steps that reduce data risk immediately:
Best Practices to Secure Data from Modification: Cyber-Attack Risk Reduction Strategy

- **Partition data** into two basic categories of “Static Data” and “Dynamic Data”. *Static Data* identifies that data which is not expected to be changed, or is changed infrequently. *Dynamic Data* is data which may need to be frequently changed. Data may be further subdivided into “Public Data” and “Private Data” so you may have *Static Public* and *Static Private Data* as well as *Dynamic Public* and *Dynamic Private Data*.

- **Implement a multi-layered security approach** to significantly reduce the risk of cyber-sabotage and protect critical data assets. Simple steps that can be taken before the attack to posture your organization offensively to circumvent data security threats are outlined in the sections that follow.

- **Prepare for the attack.** You know it’s going to happen someday. A hacker will penetrate your firewall and delete your files or someone will accidentally delete critical files or reformat your disk, and your systems will be down. Worse yet, critical data may be lost forever.

  It’s easy to tell when your data has been deleted – when you try to access the data it is gone, or your system is down and will not boot. But what if critical data was changed, something as simple as changing an account number for the destination of a wire fund transfer? Or a critical part number was changed for an airframe assembly?

  How will your business be financially impacted? What damage to your data will occur? How long will you be down? What’s the plan for recovery?

- **The best defense is a strong offense.** If it can be protected, then you don’t need to fight the battle later. You need a RRS plan in place now to avoid a disaster to begin with. Your team needs to be educated on how to protect your data and how to respond to the threat.

**Today’s Threats**

Cyber-attacks by hackers have shutdown many corporations and government agencies. It is common to hear about websites and databases that have been deleted or modified, which has caused significant outages and financial loss.

Sony Entertainment recently was attacked resulting in massive data damage and business losses with their systems having been rendered useless.

Regardless of whether your company has 10 or 10,000 computers, if they suffered data loss, could your business recover?

In one instance, data was wiped from a major oil producer causing untold millions of dollars in damages and lost revenue. This cyber-attack destroyed data on 30,000 of Saudi Aramco’s computers.

Viruses like Cryptolocker and Shamoon can exploit the presence of shared hard drives in order to delete your data and to spread to other computers on the target organization’s network. In addition to sending data to the perpetrator of the attack, Cryptolocker and Shamoon also delete files on the victim’s computers, often rendering them un-bootable with all data lost.
In other recent cases, hackers attacked several casinos which were brought down for several weeks due to data being deleted from their business systems. Law firms in Washington, DC suffered the same fate.

**Protection by Data Partitioning**

The simple method of partitioning your data into Static Data and Dynamic Data reduces the risk to sensitive data, allowing you to gain control of data that does not change and protect it from alteration, deletion, modification or re-formatting. Once Static data is moved to a true WORM (Write Once Read Many) technology, you know it is safe, and now your IT security staff can focus on protecting your Dynamic Data.

Static Data is any data that does not change, or that you do not want changed, or that you do not want to be deleted. Examples of Static Data are financial records, health & medical records, emails, securities exchange transactions, legal documents, video libraries, eDiscovery & litigation, audit logs and other sensitive files.

Partitioning your data also has the advantage of reducing the volume of data that must be backed up, thereby reducing the time required to make a backup and also reducing the cost and number of backup storage media required. By removing the Static Data from the backup equation, your data backup size is reduced to Dynamic Data only.

When migrating Static Data to WORM media, make an adequate number of Read-Only mirrors and place the mirrors in geographically separated locations in environmentally safe conditions. This technique eliminates the need to backup Static Data with your normal backup cycle.

1. **Determine how many copies of the data you need.** If it’s Static Data, then save it on WORM media for protection against data loss. You will want one or more local or remote copies for failover or disaster recovery.

2. **Identify the sources of data.** Your data may come from multiple disparate sources including video feeds, Email, documents, PDFs, SMS, legacy file systems, repositories, data bases or other sources. Make sure you have current access permissions in order to access the data when you need it.

3. **Classify your data and define retention periods.** Your organization needs to understand what rules are applied, what process to follow and the individuals responsible to ensure proper data destruction when the data retention period expires. Some data must be destroyed on a certain date due to legal hold or compliance requirements. Other data is needed forever or you may want to extend the destruction date when it arrives. You will need a permanent audit log of when the data was created and when it was destroyed. Software products exist that will automatically track and handle data destruction and produce a Data Destruction Certificate for your Facility Officers.

4. **Define policies and procedures for recovery of data.** Practice those procedures on a regular basis. Consider this as a fire drill for your data. What happens in a disaster and who does what?
Partitioning your data

Data can often be easily classified into **Public, Private, Static** and **Dynamic** categories.

The diagram below shows that **Static-Private** data presents the least risk because the data cannot be modified when placed onto WORM media. Typically few people have access to Private data. Due to the “Public” nature of **Static-Public**, this category of data assumes additional risk which is mitigated when placed onto WORM media.

The **Dynamic** categories represent modifiable data with **Dynamic-Public** incurring the most risk.

Encryption can restrict read access, but encryption does not provide any protection from deleting files, overwriting data or re-formatting a disk. You can, however, combine encryption with WORM media to provide this protection. Additionally, encryption has drawbacks in that it is cumbersome to implement, may result in slow data access, and if you lose your data encryption key, your data is inaccessible, and thereby lost.
There are many WORM solutions available to use for data protection, and each has a certain appeal depending on your application. These include Optical Media (MO, CDs, DVD, Blu-ray), Tapes, WORM Software Based Appliances and WORM Hard Disk Drives (HDD).

Optical Media have been used for many years in many forms. Everyone is familiar with CD, DVD and Blu-ray media and they are good for saving small amounts of data that are infrequently used. They range in the 4.7GB capacity range with slow data transfer speeds compared to HDD. This slow speed, coupled with a low-density disadvantage, requires a significant amount of time and effort to search and swap DVDs, especially if you have a lot of data. Their major advantage is that they are inexpensive, common and easy to use.

Magneto Optical is a form of disk drive that was introduced in the 1980s and is still in use today. Capacities are a step up from DVDs and typically range around 10GB in the capacity range. They are faster than DVDs, although more expensive. A disadvantage is that they require a special, not-so-common disk reader/writer.

Tape Media has been around since the 1960s and has survived today primarily for use in data backups. Tapes have a write-protect tab that can be switched after writing data that tells the tape drive to disallow writes to the tape. One disadvantage is that the tab can typically be reversed to allow writing over the data but there are also some permanently read-only versions available. Another disadvantage is that it is nearly impossible to search data content for large data volumes because each tape must be mounted and sequentially searched to the end of each tape, which could take days.

WORM Appliances are software applications that separate the client from the data. Client access is brokered through the vendor appliance which in turn decides who can access what. The appliance applies a set of rules and access controls to allow or disallow data read or write requests to the disks owned by the appliance. One of the problems with an appliance is that in order to access your data, you need the entire appliance and the entire set of disks, therefore it is not a good choice for mobile applications. In addition, data is typically stored in non-standard file formats which make it difficult or impossible to export your data to other systems or applications. Another issue with appliances is that if you remove one of the disks from the appliance, you can then modify or delete the data or re-format the drive, thereby bypassing the WORM protection, which has occurred in several high profile legal cases. Cost and operational complexity are also disadvantages.

WORM Hard Disk Drives (HDD) use industry standard SATA interfaces and are portable across all common computer systems including laptops, workstations and servers. They are fast, reliable and secure, and data can be immediately accessible or archived. Data protection is enforced within the disk itself and stays with the disk wherever it goes. They are an excellent choice for large volumes of data for video collections, records management, archiving, medical records, financial data, protection of data during cyber-attack and other uses where data needs to be available without compromise. WORM HDD can also be used to protect the OS Master Boot Record (MBR) and disk partition information so that a hacker cannot write over the sensitive parts of the disk while still allowing your OS to operate. WORM HDD can protect the entire disk so data files cannot be altered or deleted. WORM HDD also supports strong encryption standards.
The WORM HDD has the capability to operate in three distinct modes:

1. **Full disk protection** is the simplest operating mode for the WORM HDD. In this mode you write your data to the WORM HDD and when you want the disk permanently protected, it is then Finalized, very similar to the way a DVD works.

2. **Incremental disk protection** is used in scenarios where you have cycles where you want to write data, have it protected, then at a later time write more data, have that protected, etc. At some point the disk either fills up, or you choose to protect the entire disk by Finalizing, after which more data cannot be written to the disk and the disk is permanently protected from modification or deletion.

3. **Partial disk protection** allows an area of the disk to be permanently protected against data modification in that area only, but allows free access to the other areas on the disk. The WORMboot™ disk is setup so that the sensitive operating system boot and partition information is permanently protected. This allows the OS to operate normally but prevents a hacker from damaging these sensitive areas of the disk so your systems will remain bootable even after a cyber-attack.

---

**Shelf Life of WORM Media**

When evaluating which WORM media you should use, **consider how long your data will last on that media.** Will you be able to access the data when you need it? What’s the reliability and level of effort to access the data?

**CD, DVD** media have a relatively low-shelf life and degrade and scratch easily. They are typically mishandled and stored in non-friendly environments, often without a protective sleeve thereby reducing the expected shelf-life from 1 to 5 years.

**MO** media and **Tape** media have a somewhat longer shelf life and if handled in conditioned environments can last in the 20+ year range.

**WORM HDD** media can last up to 100 years in conditioned environments by periodically spinning up the disk drives to exercise the bearings and motors. When exercised, drive statistics can also be collected at that time to perform predictive failure rate analysis and perform early error recovery. There are software utilities available to produce error reports, alerts and automatic data recovery for **WORM HDD** libraries.

---

**Data recovery from media failure**

A **primary concern is what happens if the storage media fails?** Tapes, CDs, DVDs and disks eventually get old and fail. If this happens, how long will it take to recover your data? What is the complexity to create the data mirror and the complexity to restore? What’s the cost to your organization to be down for a day or two, or more?
For most WORM media you can create multiple images of data and they can be stored in various locations to reduce risk. If the media is stored in archive facilities like offsite Tape backup services, then it may take many hours to recover. If the mirror is an online HDD, then it can be recovered in seconds or minutes. For HDD failure, there are many companies that provide data recovery services. If, however, a mirror is made, then you will not need to use those services, you will only need to access the mirror.

Future Data Access with Mechanical Drive Units

You may need to access your data quickly and reliably in the future. A functioning mechanical device, like a Tape drive unit, a MO drive unit, or a DVD reader must exist in order to read the media when it fails. WORM HDD, however, is cable-attached and does not require a mechanical drive unit; it is in itself the drive unit. Simply by plugging in the cables, the device is immediately operational, and therefore you will not need to maintain old hardware drive units.

Tapes and MO capacities change and move on, and older capacity units fail or get replaced with new capacity units available at that time. Many are not backward compatible so you may not be able to read your media when needed in the future.

WORM HDDs use standard SATA interfaces common among all of today’s computer systems. Billions of these units are in use today and this interface has evolved from 1.5Gbps, 3Gbps, 6Gbps and 12Gbps, and will continue to evolve. And most new controllers support from 12G all the way back to 1.5G, so you can read old media. Conclusively, the WORM HDD is the best choice for any data that needs to be protected for the long-term. Due to high-speed and high-capacity advantages, WORM HDD is also the best solution if you need to search for your content.

Protecting Data with SHA-1, SHA-2 or other hashing functions

Hashing data files is a method commonly employed to determine if data has been modified. But if the data is not stored on WORM media, the data can still be modified or deleted. There is a popular belief that by using one of the common hashing functions (e.g. SHA1, SHA2) that data is protected. While it may be true in a limited number of cases where data is written, hashed and then the disk is placed under tight controls where no one can further access the disk or the data on it, use of hashing functions does not protect data from modification or deletion. Furthermore, if the data is changed and the hash value is recalculated and saved, the user may be tricked into believing that the original data has not been modified.

A simple example of a SHA1 hash value is illustrated below:

A simple line of text (message) is below:

This is a line of text to be hashed by the SHA1 function.
The SHA1 hashing function produces the following hash value (message digest):

**7FBBEB1ECEDBF0D6D28F7B437D0AE1F9C04EF522**

And with a slight variation in the message text (removed the period):

*This is a line of text to be hashed by the SHA1 function*

A considerably different hash value (message digest) is produced by SHA1:

**DB25F4B26040481E90199E5FD4AC47982E71BC4**

There are 2 major issues with assuming that SHA1 will protect your data:

1. In many cases the message digest (hash value) is saved in an accessible location for convenience. For example, in many cases it is stored in same file system or the same disk along with the message data. This means that a hacker can change the message data and recalculate the SHA1 hash value and replace it. So if the re-hashed message digest above is saved along with the altered message data, then you will never know that the data was altered. This can be eliminated by keeping the message data and message digest on separate media, with different access permissions, each handled by different trusted individuals and stored in different trusted environments with chain-of-custody measures implemented.

2. More importantly, regardless of how it is handled, *both the message data and the message digest can be deleted* or the disk can be re-formatted if they are not stored on WORM media.

**System Protection of the Master Boot Record (MBR) and Partition Information**

A common practice used in cyber-attack is the intent to render your workstations, laptops, servers and other systems unbootable. These heinous actions are done with the worst of intentions, to shut down your computer systems with massive data damage and long term outages.

By protecting the MBR and Partition Information with WORM HDD these areas of the disk are permanently protected against data modification to those areas only, allowing free access to the other areas on the disk. The WORM boot disk is setup so that sensitive operating system boot and partition information is permanently protected. This allows the OS to operate normally and for user files to be written, but prevents a hacker from damaging these sensitive areas of the disk so your systems will remain bootable even after a cyber-attack.
1. **Backup your data space.** Always make sure you have a complete backup before moving data around.

2. **Hard Disk Drive prices are inexpensive today.** Weigh the low cost of disks today against the cost you will incur if your data is lost or compromised. Determine how many mirror copies of the WORM disks that you need. WORM mirror utilities can make a one-to-one mirror or one-to-many mirrors. To provide maximum data protection for your organization, mirror disks should be maintained in geographically separated areas. If you don’t have remote facilities, third party companies will retain your mirror disks for when you need access, and some have the capability to mount the mirror remotely for immediate data access.

3. **Implement Master Boot Record (MBR) and Partition Information protection.** WORM disk boot protection is readily available to enforce write protection on those portions of the OS boot disk that would otherwise render systems unbootable if damaged in a cyber-attack. So if a hacker does penetrate your network defenses, they will be unable to destroy your boot sectors or partition information.

4. **Partition your data into Public/Private and Static/Dynamic categories.** All of your data including your publically accessible websites, documents, records and internal company data should be partitioned into data categories to help manage and reduce risk. **Public** data may include websites and other “open” data whereas **Private** data may include financial, proprietary, medical, payment card data or other sensitive information. **Static** data is the data that you do not want modified either from a cyber-attack or accidental alteration or deletion. **Dynamic** data is created or collected and may need to be changed on a regular basis.

5. **Determine what type of access controls you will implement.** You may want a multi-level access control policy to various categories of data. For example, you may not want any access controls on public data on your website, but you may wish to control access to certain portions of your website for customer access only. Further, you may want employees to access their employee records or to submit timesheets electronically online. These types of access controls are easily implemented via passwords or access keys. However, keep in mind that key management is critical for data access and it requires resources to administer. Remember to apply these access controls to your backup media as well.

6. **Identifying Your Static Data**
   A) This includes files and data that are important to both you and to your organization.
   B) Include files that should never change as well as files that change infrequently. Include even trivial data (pdf, documents, slides, spreadsheets, intellectual property, financial, emails, videos, music, etc.)

7. **Move the Static Data to WORM media.** Files can be moved with standard system utilities or dragged and dropped to WORM disks and DVDs. There are WORM mirror utilities that will create the WORM
mirrors automatically while data is being copied. Third party companies provide data migration services for large volumes of data for you so it may make sense to outsource this since it is basically a one-time event.

8. **Identifying Your Dynamic Data.**

   There are two ways to do this:

   A) You may assume everything else is Dynamic Data. This is the easy way, but will not provide the most benefit in terms of data reduction or data protection.

   B) If you want to obtain the best benefit from Data Partitioning, then you will need to do a little work.
      Check file access dates for your data space. If files have not been used for a long time, then there is a good chance they are Static and not Dynamic. If you ever need to modify them at a later date, a new version can be created even though you categorized them as Static.

9. **Encrypt data from prying eyes.** Encryption prevents unauthorized users from reading your data. It does not, however, prevent deleting data or re-formatting a disk. The best protection is to combine encryption with WORM media to prevent both unauthorized read access as well as preventing the possibility of deleting files, wiping out your data or re-formatting disks. WORMdisks™ support NIST FIPS 140-2 certified encryption techniques such as TrueCrypt (although now end of life) and Bitlocker with strong encryption support (AES-256, Serpent, Twofish and Cascades) and when used with WORMdisks™, data is protected from modification, destruction and unauthorized read access.

10. **Backup your Dynamic Data on a frequent basis.** Disk-to-Disk (D2D) backups are fast and easy to use. If your Dynamic data is critical, you should back it up regularly to minimize impact on your operations. The time and space required for frequent backups can be minimized through the use of periodic full backups, augmented by incremental backups when data changes to provide complete protection. To prevent accidental deletion or re-writing on top of important backups, ensure that the backups are made to WORM media. WORMdisks™ provide the ability to perform many parallel high-speed backups to reduce backup time.

11. **Use mirror utilities** to create one or more data mirrors for safe keeping.

12. **Test your disaster recovery procedures.** Often you think data backups are made, but later find out the hard way that backups were not successful. When a disaster strikes, many organizations find out that the data that they thought was backed up was in fact not backed up completely. Periodically test your recovery process and procedures to ensure that you are able to recover all of your important data if and when a disaster strikes. Many companies provide services to keep multiple copies of critical data off-site in a secure location.
**WORM Hard Disk Drives (WORM HDD)**

If you search Wikipedia\(^1\) for “WORM disk”, you’ll see: “In 2013, GreenTec-USA, Inc. developed WORM hard disk drives in capacities of 3 TB and greater. Prevention of rewrite is done at the physical disk level and cannot be modified or overridden by the attached computer”.

Today GreenTec has WORMdisks™ available in 500G, 1TB, 3TB, 5TB, 6TB with 8TB and 10TB on the horizon.

The 2012 CSO Online\(^2\) article “Protecting data with WORM drives” states: “Many large and mid-sized firms need to protect audit and legal data and assure it is not tampered with. Greg Machler makes the case for why WORM (Write Once Read Many) drives can solve many problems”.

“And administrators have the power to steal Payment Card Industry (PCI) and other profitable data and cover up their tracks.” “WORM drives would keep log data protected so that some corrupt administrator cannot erase the evidence he/she creates in doing illegal activities.”

More recently, a Google search for ‘greentec sony’ will reveal news articles referencing GreenTec that show:

“Virginia Based GreenTec-USA Offers a High Tech Solution That Would Have Prevented Sony Pictures Entertainment's Recent Cyber Attack”. “FBI warns of ‘destructive’ malware in wake of Sony attack”\(^3\)

**What You Can Do**

1. **Don’t panic. Keep your data online.** You can permanently protect it from damage. But this is a good time to take a look at your data usage patterns and see if you really need it all online anyway. It can be moved to archive easily if it is not needed frequently. This will reduce your operational costs to maintain the data. GreenTec, for example, offers WORM and non-WORM HDD management solutions to move your data to archive and automatically bring it back online when needed for educated decisions. GreenTec also offers WORM boot protection of the MBR and partition information so that hackers cannot overwrite those sensitive parts of the disk.

2. **You will need to be able to search for and find your data when needed.** Certain data may always be needed now, but you may be willing to wait longer for a historical records search. Government Capstone requirements mandate that federal agencies will need to save and deliver permanent records to NARA on a periodic basis. WORMdisk™ media make this fast and easy. WORMdisk™ eDiscovery solutions enable rapid data ingest, index, data classification and automated copy to WORMdisk™ media for protection and delivery to NARA.

---

\(^1\) [http://en.wikipedia.org/wiki/Write_once_read_many](http://en.wikipedia.org/wiki/Write_once_read_many)


3. **Hold periodic reviews** with key IT stakeholders to analyze threats. Determine your requirements, budget and potential vulnerabilities. Identify the risks associated with those vulnerabilities, the acceptable levels of risk to your organization and what you can afford. Implement Risk Reduction Strategies (RRS) based on your acceptable levels of risk and cost/benefits factors.

4. **Develop IT Security Policies and strictly enforce them.** Policies tend to relax over time. Hold periodic policy reviews and audits.

5. If needed, **hire a trained security professional** as a consultant. You may only need them to augment your staff, who are likely busy with their normal job functions. Additionally, a security professional is up to date with the newest technologies and countermeasures.

6. **Implement a Multi-layered security approach** to include physical building access, partitioned or compartmented work areas (for example, IT staff should not have access to sensitive locations where accounting or contracts management duties are performed). Obvious controls such as passwords, access tokens (CAC cards, PKI tokens, biometrics, etc.) provide a multi-factor authentication mechanism for providing stronger access security.

7. **Partition your data into the four data categories described previously.** By defining the four data categories of **Public-Static**, **Public-Dynamic**, **Private-Static** and **Private-Dynamic**, this allows you to handle data in a more manageable manner. Placing your **Static data onto WORM media** immediately reduces risk by preventing it from being altered, deleted, modified or re-formatted. Additionally, **Static** data does not need to be backed up frequently, thereby speeding up your **Dynamic** data backups and using less backup media.

8. **Select the right WORM media for your use case.** In a nut-shell, if you have a small volume of data and do not need fast access or content search, then use **DVDs**. They’re inexpensive and available everywhere. If you need to protect a large amount of data, search content, and need rapid access (like video), then a true **WORM HDD** is the right choice. **Tape** and **MO** are waning towards obsolescence. GreenTec **WORMdisks™** protect data with rapid access, portability and scalability.

9. **By placing Static data onto WORM devices,** in the event that a hacker does manage to penetrate through your firewalls into your network, they have no ability to change your **Static** data.

10. **Encrypt data during transmission** (SSL) for websites and other data transmission. **For secure data at rest, place sensitive data onto WORM media and encrypt the files.** By combining encryption with **WORMdisk™ media**, this protects from unauthorized read access as well as the loss of data by deletion, modification or re-formatting.

11. **Limit network access**, and control who has access, especially to wireless networks. Use wired networks whenever available. Purchase an Ethernet Push-button disconnect switch for your workstations. A good practice for when you stop working is either to shutdown your computer (no Wake on LAN), or disconnect your PC physically from the network so you can easily turn Ethernet on or off. When Ethernet is off, a hacker can’t get in and a Trojan can’t connect outward. There are
software utilities available to “virtually turn off” or disable the network and they will often create log entries for connection attempts. Or, although time consuming and lengthy, you can manually disable the network interface via Windows Network settings and re-enable it when needed.

12. **Make sure your firewalls are up to date** and make sure you **assign someone to watch the logs**. **Partition networks** into subnets and limit network access only to those systems required to perform work-related duties. Use VPNs for remote access. **Ensure that updated virus and malware protections are implemented.** Monitor attempted penetrations and be reactive. **Have a tiger team trained and ready** to rapidly evaluate the risks if an attack is detected. Have plans in-place to shutdown network access if threats or attacks are detected. When you think there may be an attack, push the Ethernet disconnect switch that you purchased as suggested above.

13. **Make sure OS patches are up to date**, especially security related patches. This sounds simple but is often a neglected process in many organizations.

14. **Implement access controls** (passwords, time restrictions), update and delete old users, and force users to change passwords periodically. Wireless networks for workstations, laptops and mobile devices should be partitioned into restricted subnets with strong network security access keys.

15. **Put a Disaster Recovery Plan (DRP) in place and backup to WORM media.** Control the physical media and backups. The last thing you want to find out when a disaster strikes is that your backups were **accidentally written over** or **deleted**.

16. **Put security log files onto non-modifiable WORM media** to prevent hackers from covering their tracks. Perform security audits and examine security log files on a regular basis.

---

**Minimize the Window of Vulnerability**

Although not always feasible, your data may be suitable for further restrictions on your Dynamic Data into Online and Offline access to minimize the window of vulnerability. If possible, keep as much Dynamic Data Offline when not in use. Some of your Dynamic Data may not require frequent access or updates. For example, if you have a specific time of day that Dynamic Data can be accessed, maybe 8:00AM to 6:00PM, then turn the system off that contains those disks at night, and turn it back on in the morning. This not only reduces the window of risk, but can also save considerable amounts of energy. There are several ways to do this:

1. The easy way is to manually turn your Dynamic Data server off and on. This can be burdensome, however, if you have many servers.

2. Power management systems exist that allow remote power control and monitoring. They can be programmed to turn servers on and off at specific times.

3. There are software applications available that enable users to request individual disks to be placed Offline, moved to an Archive and later brought back Online for user access. These are easy to use and Dynamic Data can be brought online by user demand and immediately turned off when no longer needed to minimize the window of vulnerability.
About GreenTec-USA, Inc.

GreenTec-USA is a systems technology company and a pioneer in data center modularization and optimization for servers, storage, video and secure document storage. The holder of numerous patents and industry firsts, GreenTec has over 30 years in the supercomputing industry for both classified and unclassified Government agencies. GreenTec provides products and consulting services to help companies and organizations determine the most secure, reliable and energy efficient solutions for data-centric applications, including their Low-Energy, High-Performance and Re-Configurable Cloud Block™ servers and secure storage systems for commercial and government agencies. The modular Block™ design provides easy to use “scale on demand” capability. The same Blocks are used in various platforms, from rack mounted data centers to space constrained and ruggedized mobile configurations.

GreenTec developed the WORMdisk™ in conjunction with Seagate, and provided the first WORM HDD on the market that could not be altered, modified, reformatted or deleted, either accidentally or intentionally. Data is permanently protected at the hardware level within the WORMdisk™ itself, and therefore enforcement travels with the disk wherever it goes, providing immutable chain of custody and cyber-attack protection. The WORMdisk™ works with most systems today, and it is simple to use, scalable, supports Windows, Linux, OS X and standard IT equipment and infrastructure in both standalone and rackmount configurations. It is the only Read-Only hard disk drive available, and supports NIST FIPS 140-2 certified encryption techniques. WORMdisk™ solutions range from small applications to large enterprise managed WORM HDD solutions.

About the Author

Stephen E. Petruzzo, President and Chairman of GreenTec, obtained his B.S. in Computer Science from The Pennsylvania State University in 1976 and has been working in the field of secure high-performance computing and storage technologies for over 40 years. He has worked at several large government and energy-sector supercomputing facilities and performed as a principal system architect for several large-scale Intelligence Community and DoD mission critical systems. Mr. Petruzzo founded several high-tech companies focused on the federal and private sectors and has several patents issued and pending for modular re-configurable system architectures, self-replicating storage systems, WORM technologies and advanced energy-saving computer cooling technologies. He also developed the MacKenzie-Petruzzo equation and produced 3D animations for prediction of late blight epidemics using over 1,000 computer generated disease simulations.

For comments or further information please contact: steve.petruzzo@greentec-usa.com