Durable Data for Non-IT: A Lab Manager's Guide to Ensuring Your Empower Data Is Secure and Available from Creation Through the Full Mandated Retention Period

Charlie Wakeham,[1] Dr. Cody Wright,[2] and Richard Cheng[3]
[1]Waters Asia HQ Informatics CSV Consultant
[2]Waters Australia Field Service Engineer
[3]Waters Asia HQ Informatics Technology Team Manager

INTRODUCTION

It takes time, money, and resources to generate laboratory data, so any loss of data is a direct financial loss to your regulated company, as well as a major compliance risk. Laboratory data must be secured and available to support product quality decisions, both at the time of the decision-making and for the full duration of the mandated retention period.

A regulated company must ensure its data is retained through the retention period and maintains its integrity during that time. While external assistance can be sought with activities such as backup and restore, disaster recovery and business continuity planning, archiving, system administration, and cybersecurity, **the overall responsibility for the regulated data remains with the regulated compan**y.

BACKUP AND RESTORE

Backup is defined by GAMP[1] as the "the accurate and reproducible copying of digital assets (data and software) to protect against loss of original data and subsequent accurate restoration of assets when required, i.e., restore activity, disaster recovery." It is the process of making a temporary copy of all data, as a lifeline in case of data loss from the original system. As an approximate guide, a backup should run as often as data is added or changed, so for a laboratory using their Empower™ Chromatography Data System (CDS) daily to acquire, process, and report data, the backup should be run daily.

In a networked (Empower Enterprise) deployment with data stored on a central server, it is only a single data storage location needing backup. If data is allowed to build up indefinitely on the server, in time the server performance will be degraded, and it may take more than 24 hours to complete a single backup, meaning that the next scheduled backup will be missed. Archiving is the solution to managing data storage for long-term retention and is discussed later in this white paper. Both backup and archive are needed to ensure that data endures (survives) and is available.[2]

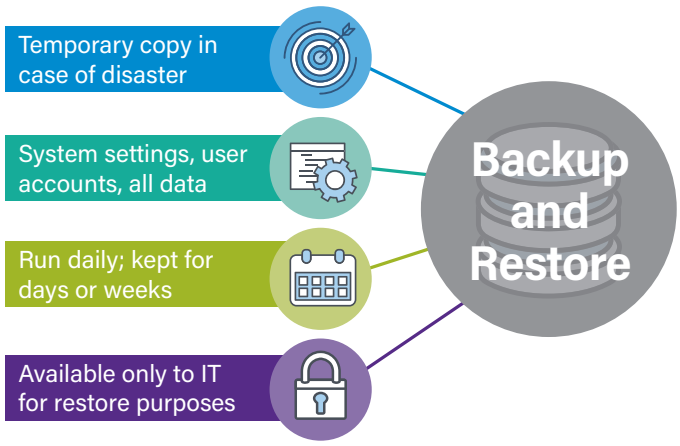

Figure 1. It is critical to run frequent backups to ensure assets can be restored in case of data loss from the original system.

Conventional backup process

For Waters™ Empower Enterprise CDS Feature Release 3 and above, backup can be scheduled to happen automatically using the Waters Database Manager (WDM) utility that is provided. With Empower Enterprise, WDM can be configured to:

- Automatically run an Oracle RMAN backup (incremental and/or full) into the Fast Recovery Area (FRA) of the server
- Automatically create a backup copy of the Empower raw data shared to a local path or network share location

QUICK TIP

Windows password expiration of the account used for Oracle jobs can result in schedule failure. Exclude this account from password expiration.

Both the Oracle database backup sets by RMAN and the raw data share backup (together referred to as backup data) will be needed to fully restore the Empower data, including system configuration (system policies settings), user accounts, audit trails, acquired and processed data, and reports.

The Oracle database can remain running while the RMAN backups are in progress so there is no interruption to Empower operations. It is essential that the RMAN backup sets are copied out of the FRA after each new backup, otherwise only the last backup is usable due to automatic overwriting of the control file. Furthermore, if the server were to fail with the only backup set still in the FRA, the original data and backup data would both be lost. Windows scheduler can be used to trigger copying of the backup sets to a separate location at a specified time after the RMAN backups have taken place.

Backup sets in FRA	Folders for every date the backup ran, containing data for the previous backups based on retention policy
	Each dated folder contains various .bkp files (full or incremental)
	Latest backup file contains the control file beginning with a "C-" followed by the database ID
Raw data share	Raw spectrum data files acquired from the instruments; contains folders with the project names and .dat files associated with them

Table 1. Components of a valid backup.

Storage of backup data

Backup data must be protected against unauthorized access, changes, deletion, and malware attack to the same level as the original data. The storage location for the backup data should be physically separate from the Empower server.[3]

Using a physical tape library or other discrete media to store backup data requires a media management plan detailing media rotation, location, security, labelling, etc.; it is essential to ensure that media are replaced before their expiry date. Consideration should be given to checking the long-term viability of the media.

A tape library can also impact the time taken to restore the data – for example, if using tapes of 20 TB capacity, it could take a significant time to locate and restore the right backup data.

Cloud storage has advantages and disadvantages as a secure location for the storage of backup data, each of which must be assessed by the regulated company. Cloud storage offers excellent security and reliability, and as off-premise storage it is likely to be immune to whatever disaster (physical or cyberattack) impacts the laboratory site. In a major disaster where the local IT infrastructure and networks are impacted however, the cloud backup may not be accessible due to loss of connection. Cloud solutions are discussed later in this white paper.

Restore process

The last full backup set and all incremental backup sets since the full backup will be needed for restoration, along with the most recent raw data share backup.

Since the restore process is most likely invoked after a data loss situation, it is vital that the restoration procedure will run flawlessly to ensure it does not fail when it is most needed. This level of assurance can only be achieved through testing of the restoration procedure.

The aim of restore testing is to verify complete and accurate data can be recovered. The scope of data verification could include checking raw data, results, methods, audit trails, system configuration, and user accounts. A sampling plan based on risk should define how many of each record type to check.

QUICK TIP

A large raw data share can make restore testing very difficult and time-consuming. Use archiving to manage your data storage and simplify your restore testing.

The restore process should be tested during computerized systems validation (CSV), at each Empower Periodic Review, and as part of testing the wider Disaster Recovery and Business Continuity Plan (discussed later in this white paper). It is important to retest the backup and restore process after software upgrades, changes to system hardware (e.g., server like-for-like replacement), and any changes to the IT infrastructure, storage locations, or backup storage medium. It is also important to test all storage mechanisms used. For example, if a tape backup and cloud backup are performed at different intervals, then they should both be tested. The test should verify the validity of the instructions in the Backup and Restore SOP, as well as the data restored.

Doing a trial restore into the production system (Empower main server) is strongly discouraged because of the risk of GxP data loss; if anything should fail during the restore, the original data in the production system may have been overwritten or corrupted.

A secondary server is an ideal test environment, if available, and has the advantage of leveraging the same IT infrastructure as the Empower main (production) server. If the regulated company only has a production server, then alternative systems must be investigated:

- With vendor assistance, and where the system is new or only contains a small amount of data, then a virtual machine (VM) on the service engineer's laptop may provide a suitable restore location. It is important that the virtual machine is the same version (FR/SR/HF) as the production server.
- Where the production server is a virtual server, a copy of that virtual server can be created as the restore location. It is important to note however that the Oracle embedded license in Empower only permits one Oracle instance full-time. If the copy (test) server is only used to host a restore test of the of the production RMAN/Raw data files backup and then the test server is deleted after test completion, there should be no requirement to purchase additional licensing.

The restore process and subsequent data verification must be formally documented.

Backup approach for virtualized servers

With virtualized servers, including cloud-based deployments, often IT preference is to capture complete images/snapshots of the VM daily, rather than schedule full and incremental backups and then manage the backup data. However, it is important to note that if the database is running when the image is taken, and a transaction is in progress during the image capture, there can be inconsistencies between what is in the computer memory and what is written to storage. This can result in the database being unstable in the restored image, in which case the database will need to be restored from the database backup sets in the FRA of the image. It is therefore important to schedule the image to be taken just after the database/raw data backup completes, so that if the Empower backups have to be restored, there is minimal data loss between the time of the Empower backup and the time the VM image was taken.

High availability solutions

High availability solutions, such as mirrored servers and transactionally consistent database copies (e.g., Oracle Data Guard), and clustering options (e.g., OracleRAC) can significantly reduce the probability of data loss and therefore decrease the chances of needing to perform a restoration. Such solutions reduce the need for conventional backup and restore processes but will require a separate Oracle license purchase as the embedded Oracle license within Empower does not cover such solutions.

When using these tools, it is important to check the release notes for the Empower version to be used to ensure that the correct database/OS/Empower versions are being used, as the certificate of structural integrity for the software is only valid for the combinations specified in the release notes. Remember that employing a Data Guard solution can only reduce the data loss risks for certain types of failures; if the servers are in the same physical location, they will still be susceptible to events such as natural disasters. Furthermore, if database corruption were to occur, it could also be copied to the redundant database. It is therefore still important to maintain adequate backups.

Waters assistance for backup and restore

Waters engineers can assist with setting up the backup routines in WDM as part of the Empower installation and configuration activities. Determining the backup settings for both the database and raw data share and setting the backup data to copy via Windows Scheduler is a regulated company responsibility. Internal verification should be performed after implementation.

Waters support for restore testing – providing a VM on a laptop (data size permitting) or a test server (check with your local Waters office if they offer this) and executing the restore against a formal test script – can be purchased as a service.

Backup and restore testing are also included as part of Waters Computerized Systems Validation (CSV) services, where assistance can be purchased to guide the regulated company through the CSV process and produce validation deliverables tailored to the regulated company's intended use.

WIDER CONTINGENCY PLANS

Backup and restore deals with the protection of a single system's data in the event that the data storage media (i.e., server) fails. A regulated company will have multiple systems comprising not just data but also hardware and infrastructure and needs contingency plans in place to deal with a range and scale of issues.

DISASTER RECOVERY PLAN

A Disaster Recovery Plan (DRP) is defined by GAMP[4] as "a sub-set of Business Continuity Management that focuses on regaining access to an IT system, including software, hardware, and data following a disaster." It is immediately obvious that the scope of disaster recovery includes backup and restore but must also make provision for replacing or restoring the whole computerized system. There should be a DRP for each computerized system within the laboratory; in the figure below only the Empower CDS and NuGenesis™ Laboratory Management System (LMS) are shown as examples.

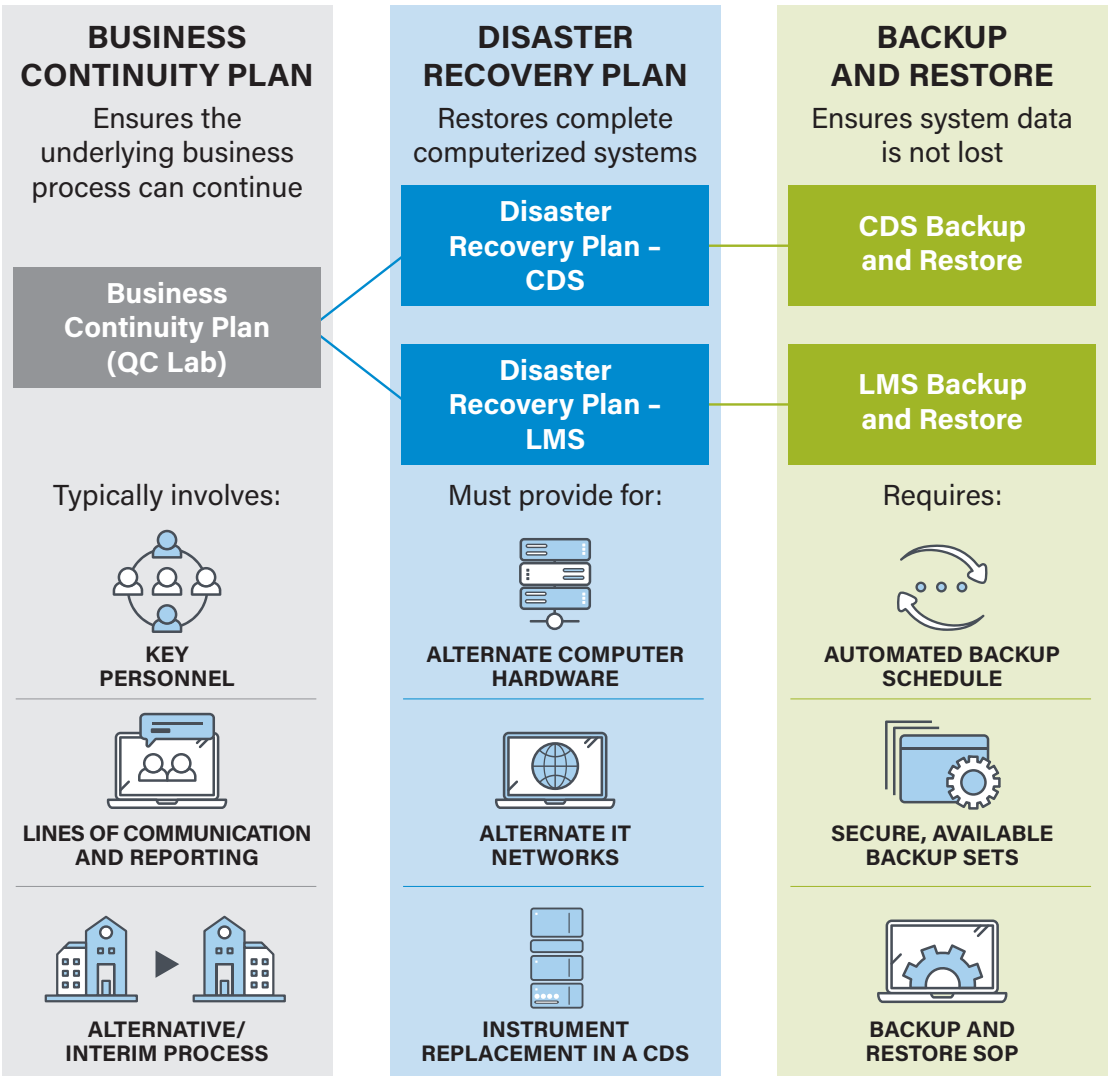

Figure 2. Regulated companies will need contingency plans in place to handle a range of issues.

Levels of contingency planning

In the case of a CDS, the system includes chromatographic instruments without which the CDS cannot function. The DRP must therefore include provision for replacement instruments, as well as computer hardware and networks. Where a regulated company uses instruments from multiple vendors, they will need to put in place service level agreements (SLAs) with each of those vendors, defining the maximum allowable period of time the vendor has to supply, install, and qualify replacement instruments.

The DRP needs to include a source of alternative computer hardware (Empower server, LAC/E, and clients for the CDS) in the event that the hardware has been impacted by the disaster.

Depending on the scope of the disaster, the IT networks may have been impacted. An enterprise system without networks is useless. If the server is onsite and it is only the laboratory LAN that has failed, then it could be feasible to re-route the enterprise traffic via the office LAN, or to set up a temporary and/or wireless LAN for the lab to use as an interim measure. However, such measures should be pre-evaluated and tested before the disaster takes place.

A larger concern is if the IT infrastructure in the geographical area has been disrupted when using Empower Enterprise over a WAN (i.e., there is no outside connection to the internet) and the server is located remotely from the site.

BC LAC/E

In the situation where the connection is lost to the remote Empower server and is unlikely to be restored in the near future, Waters BC LAC/E provides the solution to allow chromatographic analyses to continue. A BC LAC/E can operate as a regular LAC/E, providing acquisition services and instrument control within the Empower Enterprise network during normal operation. However, the BC LAC/E also has an Empower Personal database pre-installed on it, and an Empower data synchronization tool called SecureSync,™ which will copy projects templates and users to the Empower Personal database on a scheduled basis. The Empower Personal database is not accessible to users during normal operation, although it is accessible to SecureSync to allow the synchronization to proceed. The BC LAC/E in normal operation mode will operate like any other LAC/E, acquiring data and streaming it in real-time to the remote Empower server.

In the event of a disaster involving prolonged loss of connection to the remote server, the BC LAC/E can be configured by a power user to operate as a stand-alone Empower Personal workstation, which already contains project templates with methods and users associated with certain preconfigured user groups from the Enterprise database on the Empower server. The same approved methods are available for use by users with the same privileges as in the Empower Enterprise network, but without the reliance on the (lost) connection to the remote server. The BC/LACE contains 10 named user licenses for Empower Personal, and relies on local authentication; where LDAP has been used in the Enterprise system, at least one user replicated to the BC LAC/E must always be set to local login so they can change the other users to local login after the network outage.

QUICK TIP

For companies with Empower Enterprise deployed across a WAN or cloud, Waters BC LAC/E provides a way to continue laboratory analysis during prolonged network outages.

When the network connection is restored, the project data generated during the outage can be restored into the Empower server, and the BC LAC/E returned to normal LAC/E operation.

Waters assistance with disaster recovery

Waters subject matter experts can provide advice on disaster recovery approaches for the Empower Enterprise system. Waters can enter into service level agreements (SLAs) defining Waters response time for a range of disaster recovery needs, including supply of new or loan instruments and database restoration support.

The Waters BC LAC/E can be purchased and configured to act as Empower Personal in the event of a loss of connection to a remote server.

BUSINESS CONTINUITY PLAN

GAMP[5] defines business continuity management (BCM) as encompassing *"the steps required to restore critical business processes"* and notes that a business continuity plan (BCP) will *"identify the triggers for invocation of the [disaster] recovery plan, people to be involved and required communication, as well as the interim processes to maintain the process previously performed with the use of the system."*

Business continuity is a regulatory requirement for computerized systems supporting critical processes,[6] and the BCP must be documented and tested. Each company needs to design its BCP to suit its products, markets, budgets, and risk tolerance. The business continuity management approach should be based on two key considerations:

- The recovery point objective (RPO) defines how much data the company can afford to lose. This can range from the last few minutes of data being lost, to days or weeks of data. Reducing data loss drives up the cost of the backup solution.
- The recovery time objective (RTO) defines how quickly an alternative system needs to be available. Again, this can take from minutes up to days or weeks and has an associated cost.

QUICK TIP

The real RTO includes the time to locate and retrieve the backup data; where offsite physical storage is used this can significantly increase the RTO.

There may be a break-even point, where it is possible to still repeat the analysis of samples and it is more cost-efficient to re-run the samples (taking minutes to hours to do the repeat analysis) than to implement a near-zero RPO.In Figure 3, the example company has chosen an RPO on the basis that they can repeat the samples for any recent data loss but has spent additional money to achieve a short RTO because they cannot operate without their Empower System.

Each organization should define its RPO and RTO based on system criticality and the risk to data, and then work to implement a business continuity approach to support those objectives.

The actual recovery point and time should be measured during testing of the BCP and assessed against the desired objectives. With sophisticated, high availability solutions, the system and data can be 99.9% available and protected at all times, but this comes at a high cost.

Waters assistance with BCP

The BCP consists of the Disaster Recovery Plan combined with the definition of the key personnel to be involved in the disaster recovery process and the lines of communication to be maintained throughout the regulated company during that process. The BCP may even contain detailed provision for an alternative business process (e.g., switching finished product testing during a disaster from the in-house QC lab to an external contract testing lab previously audited and approved by the regulated company).

The scope of BCP far exceeds Waters Empower Enterprise and therefore Waters cannot provide assistance beyond disaster recovery.

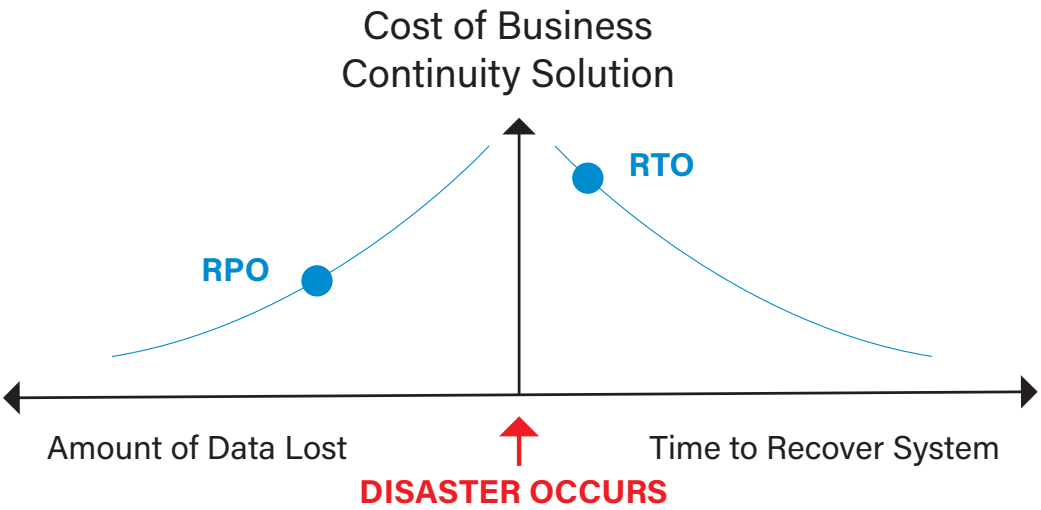

Figure 3. Example of a company's chosen RPO and RTO.

ARCHIVING

The function of an archive is to provide secure storage of regulated electronic data throughout the mandated retention period. Data may be placed into the archive as a complete data set for a specific project (e.g., method development and validation data) or at specific time points (e.g., archived monthly or quarterly for previously tested and released production batches).

The data in the archive is kept for years, with the mandated retention period depending on the type of data (see Table 2). Keeping paper records of chromatography data does not satisfy the regulatory requirement for record retention; the data must be maintained electronically in a dynamic format (able to be re-processed). This means that the original electronic data (channel data, methods, and results) must be retained since the summary report is not sufficient; it is static and only a summary of the data.

Archived data should not remain under the control of the originating department and control should pass to an independent archivist.[8] The archived data should be physically secured in a separate location from the backup data and protected against loss.

Archiving is important for the following reasons:

- It shortens the time taken for a full backup to run as there is less data to backup.
- It results in faster restore times from the smaller backup set.
- It reduces storage costs since the system can operate with a lesser server capacity.
- It minimizes backup storage costs as there are not multiple copies of the same unchanged data contained in the backup sets stored.
- It helps to maintain system performance by reducing search times and database row loading times.
- It makes navigation and searching of projects easier in the live system as old projects have been archived off.
- It limits who can access the data in the archive.

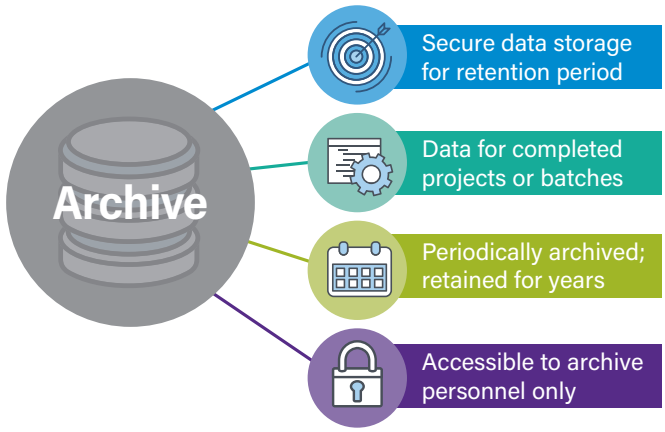

Figure 4. Archiving provides secure storage of regulated data through the mandated retention period.

Data	Regulation	Retention Period
Non-clinical laboratory studies	21 CFR 58 §58.195(b)	▪ Two years after approval of an application for research or marketing permit ▪ Five years after submission of an application for a research or marketing permit ▪ Two years following the date on which the study is completed, terminated or discontinued (when no submission to FDA is made)
Batch records for finished pharmaceuticals	21 CFR 211 §211.180	▪ One year after the expiration of the batch ▪ Three years after distribution of the batch for OTC drugs lacking an expiration date
Batch documentation	2003/94/EC Article 9.1	▪ One year after the expiration of the batch for a medicinal product ▪ Five years after completion or formal discontinuation of the last clinical trial in which the batch was used, for investigational medicinal products
Batch documentation for medicinal products	EU and PIC/S GMP Part I, Chapter 4.11	▪ One year after the expiration of the batch OR ▪ Five years after certification of the batch by the qualified[7] person, whichever is the longer
Critical documentation, such as raw data for validation or stability	EU and PIC/S GMP Part I, Chapter 4.12	▪ Retain for the duration of the Marketing Authorization
Batch documentation for APIs	EU and PIC/S GMP Part II, Chapter 6.13	▪ One year after the expiration of the batch OR for APIs with retest dates, three years after the batch is completely distributed

Table 2. Regulatory retention periods.

Manual archiving from Empower involves backing up one or more projects to a location off the server, and then manually deleting the project(s) from Empower. The Empower audit trail records the project deletion, but separate manual documentation is needed to record the archive location. When there is a need to view archived data, for example in an audit or investigation, the record must firstly be located based on the manual documentation and then the record must be restored to Empower for viewing.

Automated archiving is achieved using Waters NuGenesis SDMS Software, or the Waters Empower PLUS* DM packaged solution. Comprehensive rules can be created in the archiving template to define that projects should be copied into the archive after a set period with no activity, and whether the original project should be removed from Empower immediately after archiving or a fixed time period later. The archiving process for a project is fully audit trailed within Empower.

Once in the NuGenesis SDMS or Empower PLUS DM archive, records can be searched based on sample I.D., batch number, user, etc., and viewed directly in the archive. Note that the File Capture data is the true copy of the electronic records that must be retained as dynamic data for the regulatory retention period. Any Print Capture data captured using NuGenesis SDMS provides convenient access and viewing within NuGenesis SDMS but is not a true copy of dynamic data, such as chromatography or spectroscopy data.

QUICK TIP

Automated archiving is preferred by regulators as it can be validated to ensure all the data is archived before deletion and the archive actions will be audit trailed.

The same archiving solution can also be used to archive data from other laboratory data sources, such as FTIR, UV-Vis, TOC analyzers, etc., offering efficiency gains and data integrity assurance across multiple instruments and systems. For File Capture data originally generated in non-Waters software, it will be necessary to restore the file back to the native application for viewing and any re-processing.

Waters assistance for archiving

Waters specialists can advise on the most appropriate product for your archiving needs – NuGenesis SDMS or the Empower PLUS DM packaged solution. Waters engineers can assist with creating archiving rules (templates) for capturing data into the archive.

Waters Computerized Systems Validation services can be purchased to guide the regulated company through the CSV process and produce validation deliverables tailored to the regulated company's intended use, verifying the data integrity controls and archive functionality within the archive system (NuGenesis SDMS or Empower PLUS DM) to ensure the archived data remains complete, consistent, and accurate throughout the mandated retention period.

SYSTEM ADMINISTRATION

It is important that one or more system administrators are appointed to manage and maintain the Empower system in a compliant and functional state. There are regulatory guidances and warning letter citations around the importance of having a system administrator with no direct interest in the data generated by the system, that is, they must not be a member of the department generating or using the data. It is also important, however, that the system administrator does have competent knowledge of the Empower architecture, data flows, administration functionality (e.g., the impact of the system policies), and normal operation to ensure they manage the system effectively, as well as an understanding of the need to meet GxP and data integrity requirements.

System administration activities include (but are not limited to):

- Monitoring server capacity and free disk space
- Archiving Oracle alert logs
- Managing users, user groups, and raw data shares
- Resetting passwords and locked user accounts
- Changing system policies and user types under a formal change control process
- Deleting projects where manual archiving is used
- Archiving and restoring system audit trails
- Verifying the backups have run as scheduled and are secure

Waters assistance with system administration

Waters offers system administration training as classroom training or eLearning. It is important to note, however, that Waters personnel cannot taken on the role of system administrator for a regulated company's system.

** Empower PLUS may not be available in all regions. To discuss options for your laboratory, please contact your local Waters Informatics representative.*

CYBER CONSIDERATIONS

Leveraging cloud computing

Cloud computing offers significant flexibility and excellent reliability compared to traditional on-premise physical servers. Cloud computing can be used:

- To host a complete application in a cloud computing instance – Waters Empower CDS versions FR-4 Cloud and above can be hosted in the cloud on an Infrastructure as a Service (IaaS) basis.
- As a secure storage location for backup data.

When deciding between on- and off-premise location, consider at least the following items:

Advantages of cloud usage

- Backup data can be kept in simple storage with claims of 99.999999999% of durability.
- Access to the system and/or data requires a direct connection or VPN to the cloud, reducing the risk of unauthorized access. Direct connection, for example using AWS Direct Connect or Azure Express Route, to the respective regional data centers (or similar connection from other cloud providers) is strongly recommended as they are low latency, high performance, "private" (no internet traffic) interconnects.
- When hosting the application in the cloud, the need for physical security around the server is removed because the server is hosted in a virtual private cloud (VPC).
- Cloud solutions will generally not be affected by events that affect the laboratory site (i.e., malware, natural disaster, or directed cyberattack).
- Cloud computing resources can be scaled to fit the size and performance requirements as they are needed.
- The cloud provider effectively takes care of the hardware and IT infrastructure elements of Disaster Recovery as alternative cloud hosting resources for the regulated company's VPC are provided near instantaneously if the original instance fails.
- It remains the regulated customer's responsibility to manage backup and restore of the contents of the VPC – this can be achieved by using Waters Database Manager and RMAN to generate backup data for storage in the cloud or on-premise (or both).

Disadvantages of cloud usage

- Cloud usage relies on reliable, high speed, high bandwidth internet infrastructure, which may not be available in all geographies.
- Cloud providers rarely submit to customer audits and therefore the regulated company can only rely on the provider's own documentation for quality purposes. Some providers do offer clear statements around GxP compliance.[9]
- A Service Level Agreement will need to be instigated between the regulated company and the cloud provider, defining the security, data integrity, confidentiality, quality, performance, and support requirements that the cloud provider must meet.
- There will be additional effort to configure the way the cloud interacts with the site network, and some site network security controls may interfere with the cloud connection.
- It is essential that your company's IT have expert knowledge of cloud computing for support purposes.
- Cloud computing may be a monthly variable cost rather than a fixed capital outlay and therefore requires a different budgeting approach.

Waters assistance with cloud deployments

Waters Empower can be hosted in the cloud on an Infrastructure as a Service (IaaS) basis. It is the customer's responsibility to provision the cloud computing instances, to set up site connections, including VPN or direct connections, and to administer and manage the Empower application in the cloud (this is the same responsibility as for on-premise Empower). Once the customer has the specified instances in place with their chosen cloud provider (e.g., AWS, Azure, Alibaba Cloud, CenturyLink, Google Cloud, etc.), Waters engineers will install Empower into the cloud environment using conventional installation methods.

QUICK TIP

In a major disaster, the internet infrastructure may be lost, taking away the connection to the cloud. Waters BC LAC/E can help to mitigate this risk.

It remains the customer responsibility to provision the cloud computing instances, to set up site connections including VPN or direct connections, and to administer and manage the Empower application in the cloud (this is the same responsibility as for on-premise Empower).

CYBERSECURITY

Consideration of cybersecurity threats (viruses, malware, ransomware, etc.) is important when initially setting up an Empower network and is a key part of any business continuity plans. There are two important aspects to consider when it comes to cybersecurity:

- Prevention
- Recovery

Furthermore, if policies are already in place at the time of installation it is easier to troubleshoot then, than to deal with issues later in a system that is already in use with regulated data and needed for operational use. It also makes it easier to stick to the "most restrictive" policy, as small, incremental changes can be made to determine the exact settings needed to maintain functionality, as there is less pressure to get the system online.

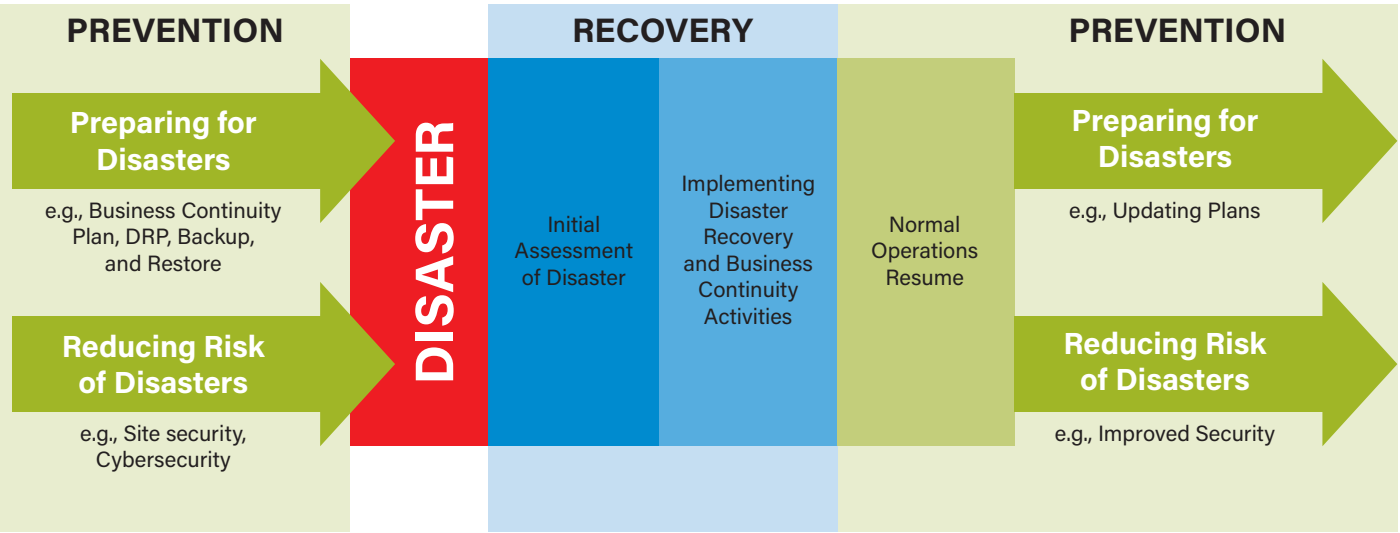

Figure 5. Prevention is preferred, but recovery plans should assume that a cyberattack has happened.

Disaster prevention and recovery

Prevention is the preferred solution, however cybercriminals are resourceful and in time may circumvent even the most stringent of security measures. The recovery plan should therefore assume that a cyberattack has happened.

Preventative measures

This is by no means an exhaustive list and a detailed risk assessment should be performed in conjunction with local IT personnel when developing a cybersecurity plan.

Plan from the beginning

Regulated companies typically opt for a most restrictive approach when it comes to IT permissions (such as firewalls, group policies, etc.). When planning a new Empower installation, it is important that these permissions and policies are in place on the IT hardware (i.e., the server(s), LAC/Es and clients) before installation begins. When the Empower installer is initially run, it will add most of the appropriate permissions required for operation.

After the installation, it may also be prudent to force a group policy update on each of the computers to be used to test if any group policies that roll out at the next policy update will interfere with Empower operation.

QUICK TIP

Ensure the IT policies and any Empower-related exceptions are documented in detail. Test any changes before implementing them into the live Empower system.

If a change in firewall or anti-virus policy is applied after the installation, it may override the exceptions the Empower installer has put in place, causing issues. Any IT policies to be changed should be fully tested on the Empower environment before roll-out to ensure uninterrupted Empower operation. The ability to roll-back the changes must always be available.

Maintain a modern operating system/Empower version

One of the most important aspect of prevention is maintaining a modern infrastructure. Unsupported and obsolete operating systems are no longer updated to cope with ongoing security threats, which increases their vulnerability to cyberattacks.

Maintaining a modern operating system and Empower version improves not only the overall security of the system but also allows the regulated company to leverage ongoing application support. Waters Release Notes for updated Empower versions list the Windows hotfixes that were applied to the operating system before the release testing took place. For those Microsoft hotfixes that Waters determines to be critical to our software applications, Waters will perform a set of regression tests. This subset of testing will only be performed on the latest version of each software package and is expected to include:

- Data acquisition
- Data buffering in a network configuration
- Benchmark calculations
- Printing[10]

The need to remain current is reinforced in the PIC/S Data Integrity Guidance,[11] which states:

"Operating systems and network components should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conduced in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system."

Minimize extraneous activities

Empower clients should be limited, where practical, to function solely for interacting with the Empower application. Activities such as browsing the internet, checking email, word processing, printing documents, or any other non-lab related activities should be restricted. Though it may seem innocuous to check emails while a sample is running, activities such as this present a risk of infection from malware, spyware, or viruses. Maintaining a separate Empower network as a closed system, and not installing unnecessary business applications on Empower clients, can reduce this risk.

If it is not practical to use Empower clients only for Empower activities, then virtualization schemes should be considered such as workspaces or Citrix with an Empower Cloud setup, or Citrix on a traditional on-premise installation. These types of measures can, to a degree, limit the spread of malicious code by not having direct access to the Empower server from the office computer.

Other physical aspects to improve security can also be implemented. This can include disabling autorun on USB drives, or disabling USB/optical drives altogether.

However, it is important to remember that rules should not impede normal workflow to such an extent that they are circumvented. Simple internet searches can often provide ways to defeat a large amount of restrictions and security features, in turn restoring or even increasing the data integrity risk originally trying to be avoided.

Do not use general Windows logins

For GxP use with Empower, it is important to have unique Empower logins as part of the requirement for actions to be attributable. Empower logins operate independently of the Windows logins and do not leverage the Windows account or username – this may have tempted some organizations to consider the use of shared Windows logins.

QUICK TIP

A shared Windows login can introduce security risks to Empower as it increases the possibility of a malicious user accessing the Empower network.

Shared logins often suffer from simpler, easier to remember passwords, which are well known to many people, and quite often can be easily guessed (if not written on the computer). If a person with malicious intent is able to access the shared Windows login, they will have access to the Empower network and may find a way to cause loss or harm to the system. Requiring individual Windows logins adds just one more layer of security to your Empower network.

Users should be encouraged to logout when they no longer are actively using the computer, as Empower will continue to acquire and store data even if no one is logged in. In a multi-user environment, fast user switching can result in many users being logged in at once. Though this may not present a specific security threat, it can consume a large amount of computer resources unnecessarily, which can cause out of memory problems with Empower. It can also encourage users to perform hard reboots if a user locks a computer and does not log off, preventing others from accessing the client. Rebooting mid-process can cause corruption to files being written at the time. If it is an acquisition computer that is rebooted, acquisition will be halted.

Recovery from a cyberattack

Once the incidence of an attack has been discovered, it is essential to identify which systems and data have been affected and when the attack started, and the specific malware/ransomware/virus involved. Generally, the recovery from a cyberattack, such as malware, will rely on the restore processes addressed at the beginning of this white paper.

Data corruption is often part of a cyberattack and therefore redundant copies of backup data should be maintained in off-site or non-networked locations separate from the on-premise backup data. This can be accomplished in a variety of ways; for instance, storing a copy to a cloud storage bucket, or copying backups to tape or some other physical media for storage in an on-site firesafe or remote location.

It is also important, when developing your restoration protocol, that the redundant backups are tested in the same way as the primary backup, to verify that the data can be brought back from the alternative locations when needed.

Some malware is designed to activate only after a specified time delay. This is deliberate so that restoration of the most current backup will restore the malware as well. It is therefore important to have the option to restore from an earlier backup taken before the initial infection, even though this may involve sacrificing the most recent data.

Waters assistance with cybersecurity

Waters software maintenance plans can be purchased to ensure your system will remain current to the latest Empower version. The software maintenance plan with qualification option will entitle you to have the IQ/OQ by SQT performed after the upgrade for no additional cost.

Waters cannot directly consult on cybersecurity, but it can assist with the development and testing of a disaster recovery plan. Waters can also help with database recovery from backup and Empower reinstallation, if needed after a cyberattack.

Waters can provide the IT requirements for an Empower installation so that policies can be designed by local IT around them.

References

1. ISPE GAMP 5 A Risk-Based Approach to Operation of GxP Computerized Systems, ISPE 2009, ISBN 1-931879-73-7.
2. EU and PIC/S GMP, Annex 11.
3. PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments PI-041-1 Draft 3, November 2018.
4. ISPE GAMP 5 A Risk-Based Approach to Operation of GxP Computerized Systems, ISPE 2009, ISBN 1-931879-73-7.
5. ISPE GAMP 5 A Risk-Based Approach to Operation of GxP Computerized Systems, ISPE 2009, ISBN 1-931879-73-7.
6. EU and PIC/S GMP, Annex 11.
7. Qualified person is replaced by authorized person in the PIC/S version.
8. WHO TRS 966 Annex 05, Guidance on good data and record management practices, 2016.
9. Examples can be found at https://aws.amazon.com/compliance/gxp-part-11-annex-11/ or https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-fda-cfr-title-21-part-11?view=o365-worldwide.
10. Waters Policy on Microsoft Hotfix Testing with Waters Software, https://www.waters.com/waters/support.htm?lid=10008020&type=TECN.
11. PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments PI-041-1 Draft 3, November 2018.

Waters

THE SCIENCE OF WHAT'S POSSIBLE.™

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
www.waters.com