Waters
THE SCIENCE OF WHAT'S POSSIBLE.™

The Importance of Business Continuity in Today's Laboratory

Zach Brennick,[1] Lori Takalo,[1] Charlie Wakeham,[2] Larry Mugavero,[1] Tracy Hibbs,[1] and Neil Lander[1]
[1]Waters Corporation, Milford, MA, USA
[2]Waters Asia HQ Informatics CSV Consultant

INTRODUCTION

In today's fast-moving and patient-centric markets, laboratory-based businesses need a plan for how to keep critical processes running in the event of a disaster. Both natural and man-made disasters can result in halted operations, financial loss, or, in worst-case scenarios, failure of the business. When human health is impacted by drug shortages, organizations can experience losses exceeding one billion dollars and find themselves answering to government agencies.

As a laboratory, your customers (internal or external) rely on you for quality control of your raw, intermediate, or API materials, and finished product testing of medicines vital to human health, making the need for Business Continuity Plans (BCP) a priority for your organization. Business continuity planning helps to ensure you can continue meeting the needs of your customers should a disaster occur. These disasters range from malicious malware and ransomware to weather and geological events, all of which can result in the disruption of global supply chains. Small and large companies alike are vulnerable to these disasters and must make plans for how they will address them.

It is critical for organizations to implement a BCP to mitigate the associated risks and to ensure that regular business operations continue for the most critical areas of operations during or shortly following a disaster. The time required to recover operations and data will depend on the robustness of the plan and the hardware and software in place. The pharmaceutical industry is particularly susceptible to disruption, with cyberattacks on the rise and hackers increasingly targeting pharmaceutical companies.

You and your business must establish how long you could endure a network connectivity disruption at critical manufacturing sites, how the laboratory operation would be impacted, and ultimately, if you are a human healthcare organization, how the global pharmaceutical and healthcare supply chain would be affected. Establishing a contingency plan at critical sites enables you to continue releasing product by allowing instruments that are typically connected to an enterprise network to be controlled at a local level and in a manner that keeps computing systems isolated and protected from potential disaster.

This paper will highlight an example of how companies can reduce the fallout of a disaster by having a BCP with appropriate hardware and software, and the recommended steps to secure future business continuity.

EXPECT THE UNEXPECTED

Any disruption in the laboratory, planned or otherwise, can have a significant effect on operations. From planned or unplanned outages to sophisticated cyberattacks and natural disasters, the potential impact on laboratories large and small can be huge. Unfortunately, the pharmaceutical industry is particularly susceptible to disruption. Of five major business sectors, pharmaceutical is the second highest priority for attacks by hackers.[1]

A key step for preparing your business is to develop a robust Disaster Recovery Plan (DRP). A DRP is a subset of a BCP, typically focusing on a single computerized system to provide a structured approach for responding to unplanned incidents that threaten an IT infrastructure and/or computerized system (including its data) and includes a step-by-step procedure for recovering disrupted systems and networks to resume normal operations. The recovery process identifies critical IT systems and networks, prioritizes their recovery time and point objectives, and delineates the steps needed to restart, reconfigure, and recover them.[2]

While it is immediately obvious that the scope of disaster recovery includes backup and restore of the system settings and data, it must also make provision for potentially replacing or restoring the whole computerized system, depending on the scope of the disaster. There should be a DRP for each computerized system within the laboratory.[3] The goal of disaster recovery and business continuity is to minimize any negative impacts to your company's operations.

Preparing for such risks with rigorous business continuity planning is taking on an increasing level of strategic importance for pharmaceutical companies, which must establish:

- How long could a laboratory go without connectivity?
- What would be the impact on the laboratory?
- Is there another laboratory where samples could be sent?
- What would be the financial impact on the organization?

Like all highly regulated industries, the pharmaceutical sector has always had to prepare for and deal with the impact of serious events. Even the smallest interruption to operations can have significant consequences, both for the company involved and the associated supply chain. Depending on the size of the organization, the cost per hour of downtime can be up to $700,000, but, on average, a business will lose around $164,000 per hour of downtime.[4] So, minimizing laboratory interruption in the event of a crisis is a business imperative.

BUSINESS CONTINUITY

EU and PIC/S GMP, Annex 11:

"Business continuity for the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g., a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested."

In recent years, the pharmaceutical sector has become a prime target for hackers, and sophisticated cyber-security attacks are on the rise. This is due to the value of the intellectual property housed in these organizations, as well as the huge volumes of data being generated and stored across networks. Several high-profile companies have already been the subject of such attacks, with losses reported to be in the hundreds of millions of dollars. Several companies have confirmed that they experienced attacks by hackers using malware known as Winnti.[5]

As the level of sophistication increases, so does the level of security and risk mitigation required by companies to combat this pervasive threat. Neglecting to develop a suitably rigorous, robust BCP can prove extremely costly, and could be detrimental when considering loss of work to competitors, supply chain failures, and health and safety liabilities. These could all add up to irreparable brand and reputational damage.

In addition to increased risk of cyberattacks, natural disasters are becoming more frequent and severe. According to *The Economist*, the number of natural disasters worldwide has more than quadrupled since 1970 to about 400 per year.[6] Some events, like hurricanes, can be forecast and tracked, meaning some real-time crisis planning can take place, but time is critical. Despite there being a small window of opportunity to plan for them, Hurricanes Irma and Marie were two of the worst to hit the Caribbean in recent times, with Puerto Rico – home to more than 40 drug manufacturers – particularly affected.

Some natural disasters, like earthquakes, do not follow seasonal trends and cannot be predicted or planned for – they occur with little or no warning. Companies must expect the unexpected and be prepared for every eventuality in order to minimize the disruption and costs to their business.

BUSINESS CONTINUITY IN THE LABORATORY

The essential attributes to maintain day-to-day operations in the event of a crisis include maintaining sample quality and retaining the ability to continue running the most important tests while safeguarding the integrity of both historic and current data generated from testing. It is therefore critical for laboratories to understand how long they can withstand any form of network outage, what the operational impact would be, and how these risks can be lessened.

What is Business Continuity Management?

'A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.'

Business Continuity Institute

The litmus test of business continuity planning within the laboratory is how quickly instruments can be reconnected and operations re-established during or shortly following the crisis, and how the supply chain will be able to withstand the disruption. Waters™ Laboratory Acquisition and Control/Environment (LAC/E™) devices can play a significant role in a company's business continuity planning strategy. They allow connected instrumentation to be controlled locally by Empower™ Chromatography Data System (CDS), helping to diminish the risks associated with a short-term unplanned outage and allowing the current acquisition to complete.

Case study: Multinational pharmaceutical company

In June 2017, a multinational pharmaceutical company was the victim of a sophisticated global cyberattack after its computer network was compromised. Other companies based in France, England, and Russia, as well as government systems in Ukraine, were also subjected to the NotPetya ransomware attack. The attack caused widespread disruption to the company's manufacturing capability, affecting both its formulation and packaging systems, as well as R&D and other operations. It took six months to recover most of its laboratories, and in total the breach is reported to have cost the company almost one billion dollars.

Subsequent to this attack, the company, working with Waters, sought to improve its business continuity plan (BCP) to withstand such disruption and implemented a Business Continuity (BC) LAC/E solution. This contingency was tested sooner than expected when Hurricane Maria struck Puerto Rico in September later that same year. This time, the BCP, including BC LAC/E, enabled the company to reduce downtime and rapidly bring a critical site back online, limiting any further damage to the company's supply chain.

Over the next year, Waters continued to work with the company's team to evolve its business continuity strategy for Waters Empower Software even further with the Waters BC LAC/E, which allows labs to switch from Empower Enterprise to Empower Personal during a disaster to quickly bring chromatographic analysis back online during an extended network outage.

The company's new business continuity strategy included:

- The remote manufacturing site must be able to operate independently for 4–6 weeks disconnected from the main Empower network.
- Agility to synchronize key data and system level information from a remote Enterprise network database to local bench level system.
- Remote manufacturing sites must be operational in 1–3 days after a disaster situation.
- Business continuity installation and qualification service for the complete solution.
- Ability to perform instrument acquisition through storage at the bench level when disconnected for an extended period from the Enterprise network during disaster situations.

The fact that this organization experienced two disasters in such a short period of time highlights the importance of business continuity planning. The lessons learned from the first event helped increase resilience to the second event, further demonstrating the value of effective business continuity planning.

CONNECTIONS AND CONFIGURATIONS

BC LAC/E systems serve a dual purpose in your laboratory. They allow remote instrumentation to be connected to and controlled by Empower Enterprise just like a regular LAC/E, and they enable secured local control for business continuity purposes. Within the DRP for Empower, the BC LAC/E System allows work to continue with minimal disruption should a laboratory lose connectivity or need to disconnect from the network in the event of a cyberattack.

Fully preparing before an issue occurs can include synchronizing key information from the Empower Enterprise database to the local BC LAC/Es. While this can be done manually, it is a time consuming and laborious process. Leveraging SecureSync,™ exclusively for Waters Empower CDS BC LAC/E systems, to ensure essential users, methods, and project structures are available in the Empower Personal database within the BC LAC/E can significantly reduce both preparation time and any risk associated with human error. The BC LAC/E with SecureSync technology allows remote manufacturing sites to be operational within hours after a disaster situation and continue to be operational for the duration of the event.

A key component is understanding both gaps and risks to your organization. Leveraging the expertise of Waters Informatics Professional Services allows you to take advantage of the world's foremost experts on enterprise CDS so you expedite your planning, training, and implementation. Involving Waters ensures you will maximize the efficiency and robustness of your strategies to protect your data and secure the pipeline of your organization.

Planning and preparation – the difference between success and failure

The key for any business is how quickly – and painlessly – they manage to establish 'business as usual' in the event of a major disruption. Ultimately, this will be determined by how rigorous the BCPs are and how well-prepared staff are to implement these plans in a timely manner. This detailed planning and thorough preparation could potentially be the difference between success and failure. The versatility of a BC LAC/E System means it can be deployed to suit your environment, whether it is used daily at the enterprise level or isolated from the network until needed. The addition of SecureSync enables you to seamlessly implement your preparedness plan.

The most rigorous BCP must evolve with the business, in order to keep up with – and ahead of – the major threats businesses are exposed to today. While natural disasters are beyond anyone's control, malware and ransomware attacks are evolving at an increasing rate, so it is crucial that plans evolve with them. Continuous planning and analysis and thorough preparation will help to keep plans as resilient and rigorous as possible, using the following steps:

- **Business analysis** – A detailed analysis of operations will help to identify areas where the business is vulnerable. Once these are known, it is important to evaluate what the likely impact on these areas will be in the event of an attack, and ensure the plan specifically addresses these weaknesses.
- **Risk assessment** – Identify the events that pose a risk to the business and evaluate how likely these events are and the impact they can have. Consider the steps that can be taken to manage these risks and understand the impact of a worst-case scenario.
- **Strategy development** – Develop the strategy in line with the risks that have been identified and how these risks will be managed. Consider how to respond to risks that cannot be reduced, and where necessary, consult with business continuity specialists to help manage these areas.
- **Plan development** – Identify the key areas of responsibility in the event of an incident and define clear roles of who should do what from a strategic, tactical, and operational perspective. Ensure these are clearly communicated so that everyone knows the role they play.
- **Plan rehearsal** – Use regular, documented, rehearsals to test the plan to identify any holes or additional areas of vulnerability. Ensure these are addressed immediately and that the plan is refined and updated according to your procedures. Communicate any changes to everyone affected.

While preparation is critical when the time comes to invoke the plan, successful business continuity also relies on the ability to rapidly switch to an alternative method of working when disruption hits the lab. Implementing Empower BC LAC/E systems with SecureSync technology enables you to quickly invoke either a proactive or reactive disconnection approach. The nature of the situation faced will almost certainly influence such decisions. For instance, a hurricane can be predicted, so proactive disconnection of instruments can be managed, and alternative testing plans can be enacted in advance. Cyberattacks and network losses are much less predictable, and thus require a more reactive approach.

BUSINESS CONTINUITY CHECKLIST

Here is a suggested checklist to help you get started on your business continuity journey as you work to mitigate risks and keep instrument downtime to a minimum in the case of a crisis:

- **Prioritize critical sites and systems** – When disruption hits, priority must be given to the critical areas of the business. Establish priority sites that are fundamental to the operation and ensure the most vital instruments are protected. By doing so, you can plan for how to cope when one or more sites/systems go down.
- **Informed decision-making** – Build critical decision-making criteria into your planning and identify the important measures for knowing when to invoke/revoke business continuity. Clearly communicate these criteria to decision-makers with authority and ensure they are fully empowered.
- **Integrated planning** – Ensure your business continuity plan (BCP) is fully integrated into your overall business operations and procedures, and that any changes made will automatically filter through to these areas of the business.
- **Forward thinking** – Think ahead and ensure you have a BCP in place before considering any future IT investments like server upgrades or new versions of software. Work with Waters to proactively plan and identify opportunities to strengthen and streamline your Empower DRP as part of your laboratory's BCP.
- **End-to-end planning** – Evaluate all aspects of your laboratory's operations and ensure plans are in place that cover the entire process, from initial set-up through to data reconciliation.
- **Critical systems support** – Identify your operation's critical systems and know which configurations must be supported. Put plans in place to routinely monitor critical systems to ensure that they are in a state of constant readiness.
- **Operational elements** – Ensure you have your business continuity operational elements in place and embedded within your standard operational procedures (SOPs). Review these plans on a regular basis and update accordingly.
- **Training** – Ensure that the team responsible for deploying your BCP is trained, including proper training of the appropriate teams at the local level within critical manufacturing sites. On a regular basis, execute an internally staged trial BCP "fire drill" to test the execution knowledge of all teams involved, compliance to the plan, and uncover potential problems to make improvements prior to having to rely on the plan during an actual BC event.

As a part of planning it is imperative to establish at which point disaster recovery procedures are invoked and the criteria for reconnection to the network. Full enterprise operations can be resumed when the disaster has been alleviated. The timing of these decisions is absolutely critical to the effectiveness of the BCP. Waters Informatics Professional Services can help you assess the options in determining what makes the most sense for your organization.

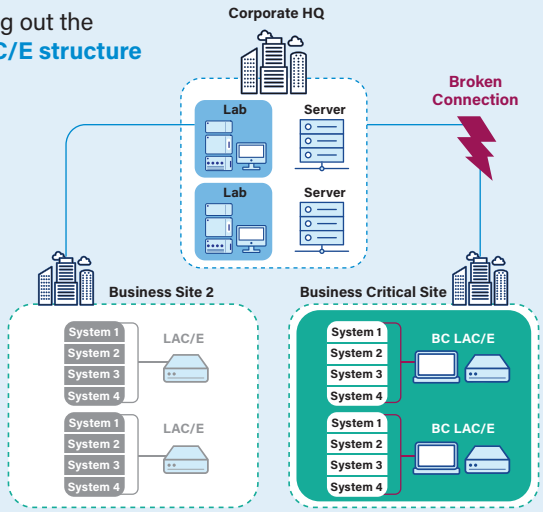
A COMPELLING BUSINESS CASE

The business case for preparing a robust plan against these threats and the impending disruption caused is a compelling one, given the impact that can be felt when a lab experiences unplanned downtime. According to Morgan Stanley,[7] climate disasters have cost the world $650 billion over a three-year period. Meanwhile, estimates suggest the loss of a pharmaceutical manufacturing site to cost between $1–2 million per day.

In the case of a multinational pharmaceutical company, although most operations were restored within six months, the company reported that the ransomware attack had a $260 million impact on sales alone. Add to that an estimated $330 million impact on marketing, administrative expenses, and production costs, and a $200 million impact on 2018 sales through residual backlog. The lessons learned by this organization after the initial ransomware attack, and the combination of the business continuity planning, engaging Waters Informatics Professional Services experts, and BC LAC/E systems, contributed to the resilience the business demonstrated when Hurricane Maria struck. If BC LAC/E systems had been in place as part of the company's business continuity planning strategy prior to the attack, the business impact and financial losses would almost certainly have been reduced.

This was not a unique situation. The pharmaceutical sector and other laboratories with intellectual property are highly susceptible to cyberattacks and all laboratories must be able to respond when natural disasters occur. Implementation of Waters solutions that include BC LAC/E systems with SecureSync and Informatics Professional Services should prove to be an overwhelmingly positive return on investment for organizations.

Mapping out the **BC LAC/E structure**



A Waters LAC/E is a purpose-built appliance designed for network installations of Empower Chromatography Data System to perform instrument control, data acquisition, remote processing, and data buffering activities – all while providing enhanced raw data security, robust remote access to instrument systems, and consistent system performance.

Implementing BC LAC/E systems with SecureSync within a laboratory's BCP, in conjunction with leveraging Waters Informatics Professional Services, can deliver several business benefits:

- **Effective planning** – Planning that is tailored to your organization's needs and tested to ensure it is robust.
- **Built for business** – Designed to deliver high levels of reliability, with no moving parts in the appliances, and the ability to prepare at the site or system level.
- **Dependable** – Rely on 24/7/365 dependability for uninterrupted supply chains.
- **Peace of mind** – Rugged and durable appliances in conjunction with trusted expert planning, advisory, and support services ensure that your organization is in an ever-ready state.
- **Reduced costs** – Each BC LAC/E comes with a four-year hardware repair/replacement warranty.

CONCLUSION

MAINTAINING BUSINESS AS USUAL

With the increased pressure to reduce costs and time to market and the need to secure and protect global supply chains, investing in technology infrastructure to ensure operations can continue at needed capacity is imperative. The proper planning adds peace of mind should your organization need to invoke your BCP. Waters has a team in place to help you with both proactive and reactive elements of business continuity planning, testing, and implementation. BC LAC/E systems with SecureSync, in conjunction with your BCP, offer a structured approach for responding to unplanned incidents and helps to minimize the impact of being disconnected.

References

1. Keown, A. More hacks inevitable in pharma industry, cyber-security expert says. *BioSpace* [Online], **2019**, https://www.biospace.com/article/hacking-continues-to-be-a-concern-for-pharma-cybersecurity-expert-says/.
2. Chardon, J. and Bassard, G. Waters' Software Disaster Recovery Plan for Business Continuity. Waters White Paper, **2016**, https://www.waters.com/waters/library.htm?cid=511436&lid=134919204.
3. Wakeham, C. et al. 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. Waters White Paper, **2020**, in production.
4. Down-time: Why you must know this number to keep your business up and running. *Jump Start Technology* [Online], **2019**, https://www.jumpstarttech.com/downtime-number-you-must-know/.
5. Roche confirms cyber-attack from Winnti malware. *European Pharmaceutical Review* [Online], **2019**, https://www.europeanpharmaceuticalreview.com/news/95107/roche-confirms-cyber-attack-from-winnti-malware/.
6. Weather-related disasters are increasing. *The Economist* [Online], 2017, https://www.economist.com/graphic-detail/2017/08/29/weather-related-disasters-are-increasing.
7. DiChristopher, T. Climate disasters cost the world $650 billion over 3 years – Americans are bearing the brunt: Morgan Stanley. *CNBC* [Online], **2019**, https://www.cnbc.com/2019/02/14/climate-disasters-cost-650-billion-over-3-years-morgan-stanley.html.

For more information on Waters BC LAC/E solutions, please visit www.waters.com/empoweryourbusiness**.**

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