

IT SOLUTIONS

# WELLINGTON



## NETWORK SERVICES

WITH SOME CREDIT UNIONS  
PROCESSING 800,000  
TRANSACTIONS ANNUALLY  
AND MOVING OVER €500 MILLION,  
SYSTEM UPTIME IS CRITICAL.

Your Credit Union information is irreplaceable. Data loss can result in downtime, loss of member confidence or worse – it can put you out of business completely. Installing systems to ISO27001 security standards, with offsite replication, automatic failover servers, encrypted back ups, proactive monitoring of your onsite systems and disaster recovery equipment for immediate deployment in emergency premises, Wellington IT Solutions have a suite of services to ensure business continuity for your Credit Union.

## KEY FEATURES

- Safeguard your Credit Union, your data and your Members
- High levels of customer satisfaction
- Quick response time
- Networks configured to comply with ISO 27001
- Comply with regulatory environment and auditing inspection
- Comprehensive testing with written reports available
- Continual daily data back ups
- A structured approach to disaster recovery, business continuity and network support all integrating with your core system
- Fully comprehensive package addressing time to recovery and data integrity concerns

---

Peter Knight  
E: [pknight@well-it.com](mailto:pknight@well-it.com)  
M: 00353 867709126

Andrew Hagan  
E: [ahagan@well-it.com](mailto:ahagan@well-it.com)  
M: 00353 867709127

T: 0044 28 9068 1531  
F: 0044 28 9066 0181

[www.well-it.com](http://www.well-it.com)

## You get a call at home; the Credit Union building has been destroyed by a fire. The server is destroyed and all Member data on it lost. You have a back up tape somewhere but you are supposed to open in the morning. What will you do?

Contact Wellington. This is a classic example of when to turn to your offsite replicated data. Wellington can replicate your Member data offsite continuously to our secure data centre. Spare equipment will be provided to help with the Credit Union's Business Continuity Plan in a disaster scenario. We will test the data replicated off site once per quarter to ensure everything is operating correctly, with a written report provided for you and your Board after each test as tangible evidence of good practice by the Credit Union.

In the example above we connect to the data center and begin the transfer of your data on to a temporary server.

The offsite backup runs constantly during the day so this data will be fully up to date. This machine can then be brought to a temporary location nominated by yourselves along with counter machines, printers, switches, cabling etc. We aim to have the site running again in this recovery setup within 24 hours.

We will then execute longer term planning; when will it be possible to get back into the original premises, what equipment do we need to replace etc.

*(Products used:  
Wellington Offsite Replication)*

## Your PC has just crashed. You have spoken to the support desk but it seems unrecoverable. You had a lot of documents saved on the PC and the payroll software is on there. It could be up to a week before a new machine will be ready and all data may be lost. How could you have avoided this?



All is not lost, contact Wellington. In our standard network configurations all documents are stored on the server only. This means that even though a PC has crashed the end user can relocate to another machine (even in a different office) and when they log on they will see their own desktop and all their previously saved documents.

Important PCs, such as those with Payroll software installed, will have an image taken of them to allow quick restoration. The faulty PC may be replaced with another PC in the building or a new machine. The backup image is then applied to this leaving the Credit Union with all programs of the PC that failed.

*(Products used:  
Wellington advanced network  
configuration, Swap and Save)*

You are going to a conference and will be out of the office for a few days. You will call in while away to make sure things are going ok but the Assistant Manager is on holidays this week and you are worried in case something major will happen. Is there a way that key members of staff in the Credit Union can be notified of issues as soon as they happen, even if out of the office, rather than having to wait until staff in the Credit Union contact them? Ideally can Wellington be notified and begin working on the issue immediately?

Notification of significant events in the Credit Union can be sent to key members of staff via email or even text message. For example alerts can be sent for things such as temperature extremes in the server room, power problems, backup failure, replication problems, EFT files not sent, website transactions or registrations awaiting authorization.

These alerts will be sent to Wellington also. Wellington also monitor CPU load,

memory usage, disk space, RAID configurations and other potential errors such as problems with fans or power supplies.

When Wellington detect a critical issue they will contact the Credit Union and work with you to resolve the problem.

*(Products used:  
Network maintenance with proactive monitoring and support, Locus Mobile)*

It has been a busy few days, there is a Board Meeting in 3 hours and you have just accidentally deleted the document you promised them and worked on all weekend. You know you should have been backing it up as you went along but you didn't. The meeting is in a few hours what will you do?

Using Wellington's Windows offsite replication solution, we replicate documents, spreadsheets, and so on over a secure channel to our data center. If you delete a document by mistake or need to recover it for any reason this is simply done via our secure website. You simply browse to the page and choose the file and version of the document to recover.



As standard 7 days files are stored, with 3 versions of each file per day. This can be adjusted on customer request.

*(Products used:  
Wellington Windows Offsite Replication)*

The Assistant Manager has just arrived and has left his laptop on the train. He had been working on some reports last night and has personal details of all current borrowers saved on the laptop. He wants to know what to do, what do you tell him?



This is serious but could be much worse. All laptops on site are fully encrypted. If lost or stolen it is not possible to access the encrypted data, limiting the security breach. All data on the laptop is stored on central servers in the Credit Union limiting data loss.

*(Products used:  
Laptop encryption, Wellington  
advanced network configuration)*

A busy Friday morning and the system is down. You have spoken to support and they say it is a multiple hard disk failure. They have tried to fix the machine remotely but it can not be done. An engineer is on the way with replacement hard disks but it will take several hours for the engineer to arrive and when the engineer is finished the server must be reinstalled and data recovered from the last backup. This will require more than a working day to complete. What could have been done to avoid this?

When recovering from a disaster there are two main concerns, recovering your data and speed of recovery. In the fire example mentioned earlier, offsite replication was used as this is the best possible protection of your data and ideal if the entire building is inaccessible. In this case, you have had an isolated issue with the server and speed of recovery is the main concern. Offsite replication is not the best solution here, as the offsite data will have a slower recovery time. Failover servers onsite will give a much faster recovery and be a better solution in this example.

Wellington install two servers in the Credit Union. All data is replicated from one server to the other in real time. If there is a problem with your primary server the system will automatically failover to the second machine. A user of the system will have minimal disruption during this process, they may have to log out and log back in. A Linux machine should failover in under 3 minutes and a Windows machine even faster.

*(Products used:  
Automatic failover servers)*

## What once seemed to be a huge computer room has now become cluttered and seems to be filling up with servers. The number of machines in there is making the room quite hot and running them all is becoming increasingly expensive. Can anything be done to reduce the number of servers in use and make things more efficient?

Rationalising the number of machines in your computer room is possible using a process called virtualisation.

Virtualisation means running software in a virtual environment. This is when the software is emulated rather than being run on a physical machine. Several virtual environments can be run on one physical server. Domain controllers, file servers, mail servers and support PCs can all be virtualised in this way.

By reducing the number of machines power consumption, carbon footprint, noise and heat will all be reduced. This also reduces the number of machines to be maintained and kept in valid warranty. Overall, virtualisation can help reduce the costs of IT ownership and simplify your disaster recovery and business continuity planning.

*(Products used: Virtualisation)*

## Things have been difficult with a few members of staff for a while now and one has just been let go. This has led to a lot of bad feeling and she still has a number of friends in the office. The Board are worried about a security breach. They want you to prevent this but what can you do?

With a secured network there are limitations on what any staff member can do. All PC's are protected to prevent the use of memory sticks, portable hard drives, burning CDs or other methods of taking data offsite. Wellington can, if required, monitor outgoing Credit Union email traffic and restrict internet access so that web based email accounts can not be used. The network itself is only accessible using a unique password in conjunction with a Staff smart card. This gives full traceability of who is on the network and controls what they can see and do. This is linked to your banking application role codes to ensure controlled access to Member data, enabling full access



control across the entire Credit Union IT infrastructure.

*(Products used: Wellington Security Pack)*