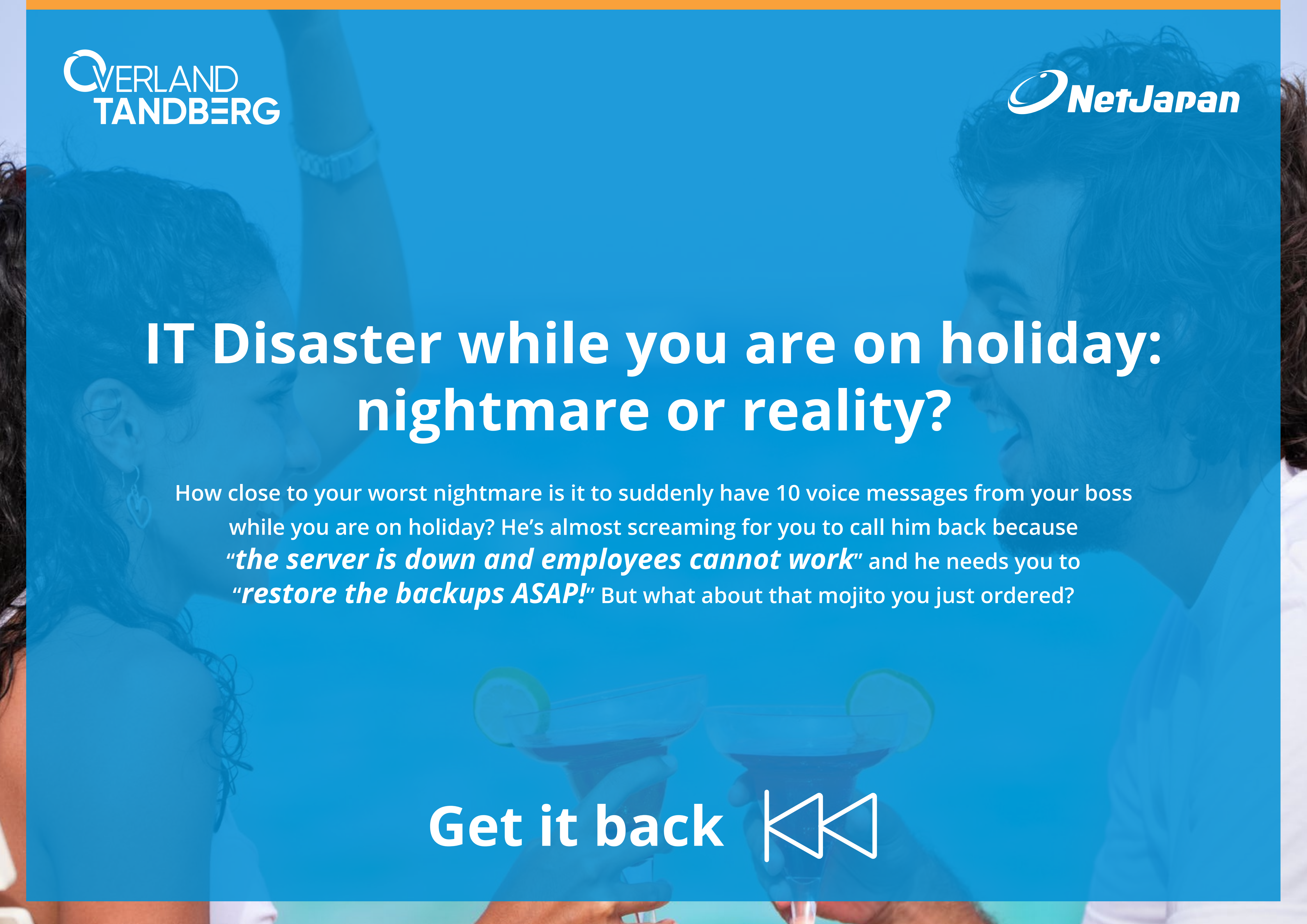


OVERLAND TANDBERG

NetJapan

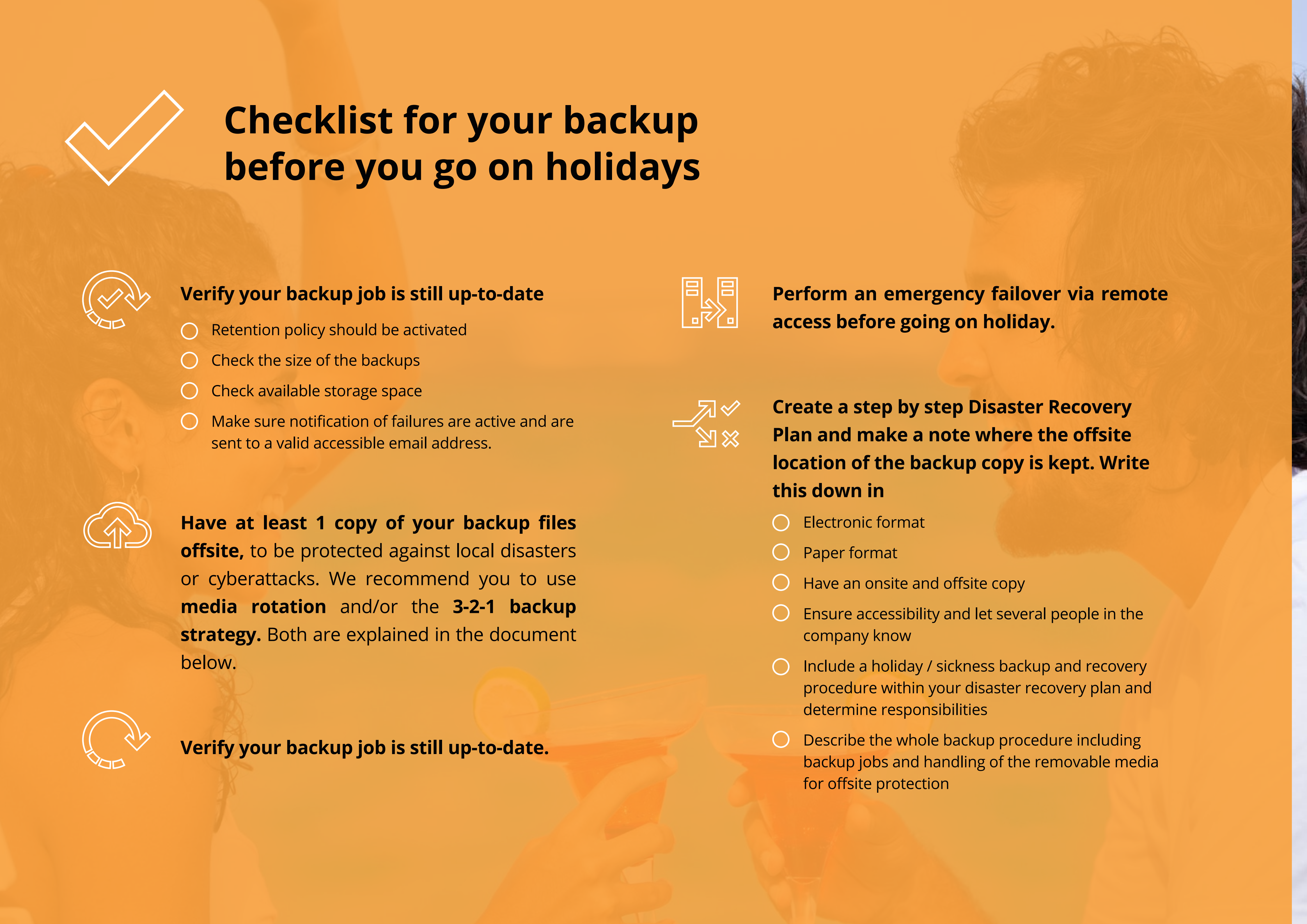
IT Disaster while you are on holiday: nightmare or reality?

How close to your worst nightmare is it to suddenly have 10 voice messages from your boss while you are on holiday? He’s almost screaming for you to call him back because “***the server is down and employees cannot work***” and he needs you to “***restore the backups ASAP!***” But what about that mojito you just ordered?

Get it back

Everyone looks forward to a well-deserved break from work while on vacation. SMBs often have 1 person looking after their IT or even just their backups. So how can you, as an IT Professional or person in charge of the backups, in the event of an IT disaster or cyberattack ensure this also applies to you?

Not relevant to you? How confident are you that your company is safe and Disaster-Ready even when you are away from the office? We know of so many stories were things went wrong and it was just too late! So what measures should you or the IT professionals take to limit the impact of disasters before going on holidays?



Checklist for your backup before you go on holidays

Verify your backup job is still up-to-date

○ Retention policy should be activated

○ Check the size of the backups

○ Check available storage space

○ Make sure notification of failures are active and are sent to a valid accessible email address.

Have at least 1 copy of your backup files offsite, to be protected against local disasters or cyberattacks. We recommend you to use **media rotation** and/or the **3-2-1 backup strategy.** Both are explained in the document below.

Verify your backup job is still up-to-date.

Perform an emergency failover via remote access before going on holiday.

Create a step by step Disaster Recovery Plan and make a note where the offsite location of the backup copy is kept. Write this down in

○ Electronic format

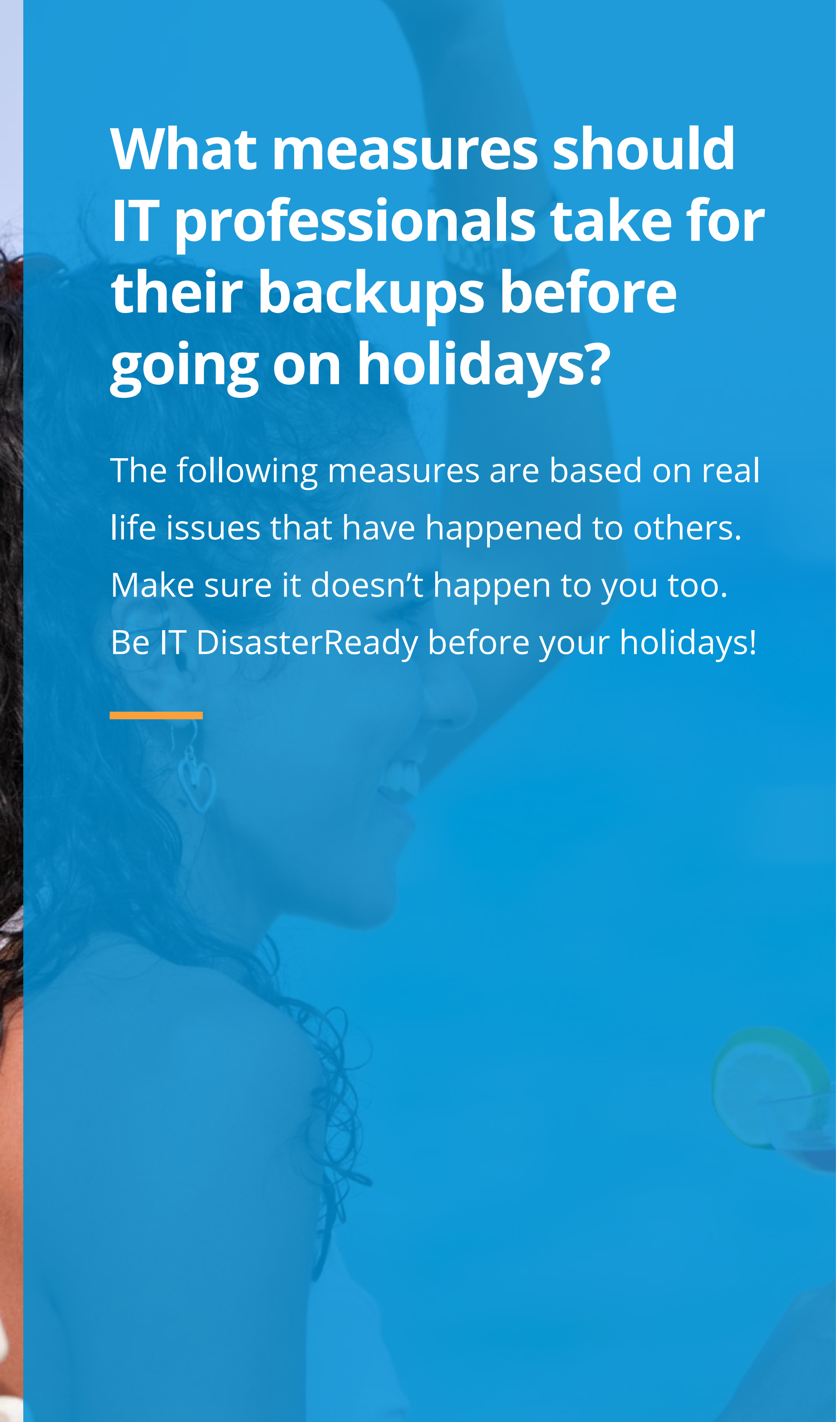
○ Paper format

○ Have an onsite and offsite copy

○ Ensure accessibility and let several people in the company know

○ Include a holiday / sickness backup and recovery procedure within your disaster recovery plan and determine responsibilities

○ Describe the whole backup procedure including backup jobs and handling of the removable media for offsite protection



What measures should IT professionals take for their backups before going on holidays?

The following measures are based on real life issues that have happened to others. Make sure it doesn't happen to you too. Be IT DisasterReady before your holidays!

Have a Backup and Disaster Recovery Plan

Write down your Backup and DR Plan and communicate it to your colleagues, your management and make sure you have a printed copy of it in case all machines are inaccessible. 40% of companies do not have a documented Disaster Recovery Plan! Don't be one of them.

○ Implement the 3-2-1 backup strategy

To ensure a full protection against IT disasters, it is recommended that companies implement the 3-2-1 backup strategy, with one storage device for the primary backup and another one as a secondary backup target. If one of them fails, the backup stored on the other storage device is still available to recover your company's data and system. In addition, a third copy of the backup chains should be stored on a removable storage device.

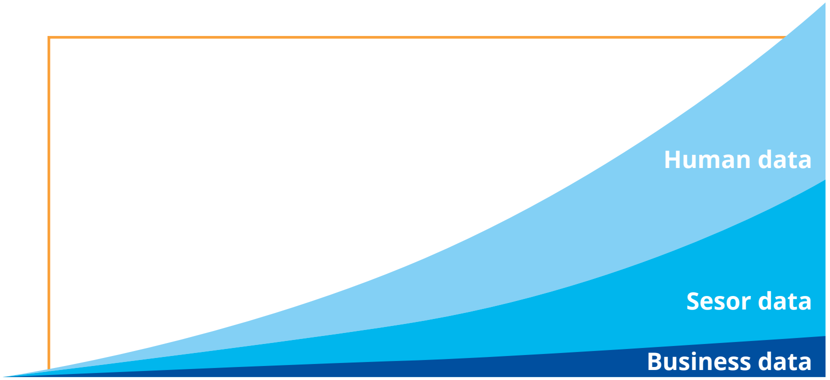
○ Include a worst case scenario

Incorporate to your DR Plan the worst case scenario you can think of. For example, a cyberattack encrypts your system and data while you are on holidays, and the person meant to rotate the external storage devices is sick! The chance for this to happen are extremely rare but when Murphy's law strikes while you are meant to relax, you the IT Professional still needs to be in control of the situation!

Ensure fit for purpose local backups

Review the free storage space that is still available

Data generation grows exponentially at x50 year on year. SMBs sometimes fail to check what their data growth rate is and realise too late that their backup storage devices are full, leaving them very vulnerable.



Check the retention policy is active and up-to-date

Retention ensures older backup are deleted or moved in order to make space for new backup files. Ensure this option is activated (if it is part of your backup solution) as it is usually not activated by default. Calculate how many backup sets (full backup with its legacy incrementals) can be safely kept without exceeding the storage capacity of your backup device.

Do not miss failure notification by being notified on everything

If you set to receive all successful and failure notifications it becomes very easy to miss a failure notification and to overload the log files. Notification should be only set for failure. And then if a backup is not created because of lack of storage, it’s easy and fast to identify and solve the issue.

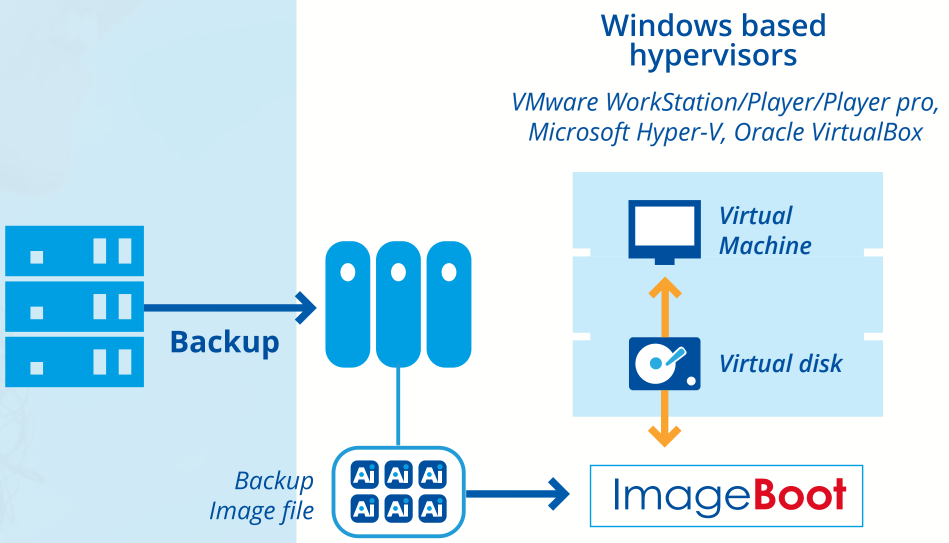
Test your backup files!

Why should you test your backup file?

Hardware or bad block failure of storage devices are not a rare occurrence over time. It can cause data loss or corruption of any of the incremental files without you being notified. If the damaged incremental backup is located in the middle of your backup chain, you won't be able to restore any of the subsequent backup files, even if you did not receive a failure notification from your backup software.

Backup verification is good, backup recoverability testing is better!

Some backup companies offer a verification feature to check the entire backup chain. This feature checks that each block of each backup file is readable. This process takes a long time and hence allot of companies choose not to activate it, but it is more secure than just having MD5 checks.


Windows based hypervisors
VMware WorkStation/Player/Player pro, Microsoft Hyper-V, Oracle VirtualBox
Virtual Machine
Virtual disk
Backup
Backup Image file
Ai Ai Ai
Ai Ai Ai
ImageBoot

However, even verification processes do not guarantee you will be able to restore your backups should a disaster strike. Why? Because it only ensures backup files are readable; it does not check block content - for example, if the partition table is broken, MD5 and verification checks may be successful but you still would not be able to boot your restored machine (yes, you can try to repair the partition but this increases the companies downtime).

Virtualisation technologies such as ImageBoot included in NetJapan ActiveImage Protector Backup and Disaster Recovery solution (for Windows and Linux) has made backup testing quick, easy and accessible for every organisation. It allows IT professionals to boot backup files (from physical or virtual machines) to virtual environments in less than 5 minutes and you the IT Professional can see with your own eyes that the machines are up and running.

Advantages of backup “recoverability” testing vs backup verification

- **Reliability:** Prove and see with your own eyes that the selected backup files boot, thus ensuring that the chain up to that point is safe and reliable.
- **Speed:** reduce backup testing time to a few minutes.
- **Frequency:** as it only takes a few minutes, you can verify your backup chain every week or even more often.

Trust is good, Control is better

Automate your backup recoverability tests to save time and make sure backup testing still happens while you are on holidays.

Very few backup vendors offer automated backup “recoverability” tests. ActiveImage Protector does since June 2017 and notifies you on failure. It automatically boots the last created backup file as a virtual machine in Hyper-V. VMware and VirtualBox support will follow soon. It automatically removes the created machine so you do not need to worry about the storage space usage.

Keep control of offsite backup copies

Network data and backup encryption from ransomware attacks are a recurring theme of the last years with CryptoLocker and more recently WannaCry and Petya attacks. Once your backups have been encrypted, it’s impossible to use them for restore. That’s why it is important to implement the 3-2-1 backup strategy mentioned earlier in this document.

Control offsite storage media schedule

Tape or removable USB drives are commonly used in SMB environments for media rotation. This might become an unreliable tool when you are on holidays.

Most backup applications are able to automatically eject removable disk technology media such as Tandberg Data RDX QuikStor, when backups are completed. It allows IT professionals to have a visible control of the backup status. It also sends a reminder to remove the media in order to keep it offsite.

In addition Overland-Tandberg Data also offers an alternative solution, the RDX QuikStation, a removable disk appliance with 4 or 8 RDX drives. QuikStation provides various operational modes. Choosing the disk autoloader mode allows performing an automated rotation through all slots optionally without manual intervention. This is helpful during holiday times if no responsible person is available or the responsible person is sick.

Maintain consistent and recoverable Cloud hosted backups

When storing your backup files in the private Cloud, do not forget to install NetJapan`s free ImageCenter LE at the remote location and activate the automated backup testing feature. Alternatively, you can conduct regular live testing of offsite backup chains using the free ImageBoot installer: it only takes 2 minutes to boot your chain in a VM!

Using public Cloud can make it trickier to check the usability of offsite backup files. That’s why it is important you test the recoverability of your backup files before they are replicated.

Make sure you can remote access to realise an emergency failover

Data generation grows exponentially at x50 year on year. SMBs sometimes fail to check what their data growth rate is and realise too late that their backup storage devices are full, leaving them very vulnerable.

Realise an emergency failover

ImageBoot is a failover solution included in ActiveImage Protector. It allows you to boot an emergency virtual machine in Hyper-V, VMware or VirtualBox using the selected backup file.

Before going on holiday, make sure ImageBoot is installed on a couple of machines of your network (not just on your critical server, in case it crashes or gets hit by an attack) and check that you have access via remote access. When you boot the image, backups can even continue to be created to the same storage device as long as you configure the backups (while in failover mode) to go to the same location. Test it before you go on holiday, it will only take you 2 minutes!

However, it is important to remember failover technologies is for emergency case only and it is not recommended to leave your company running on a failover system forever, even if it is installed/booted on a very powerful machine. A classical restore will be needed at some point. ImageBoot failover procedure helps your company to resume its activity in only 5-15 minutes and allow you to continue enjoying your holidays. You can then operate the classical restore from the Tandberg RDX drives.

Restore once back from holiday if possible – or via remote access otherwise

If the company can continue running on the emergency failover machine for the rest of your holidays, then relax and enjoy the rest of your holidays and have that mojito.

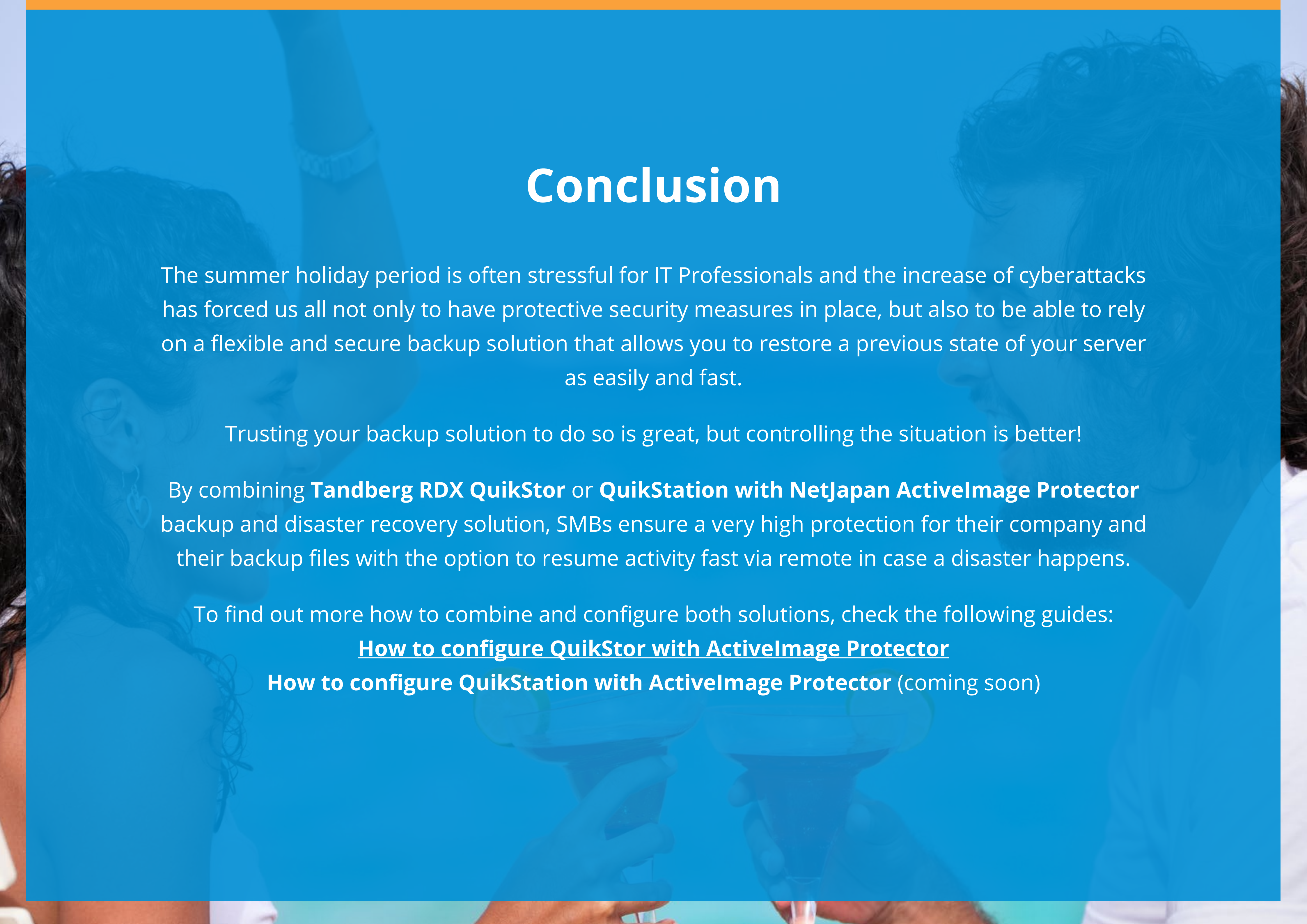
Otherwise, connect to ActiveImage Protector Recovery Environment with a remote connection and use the Recovery wizard to restore the failed machine. In the meantime, employees will continue working from the failover VM.

In case of hardware failure, try to organise the replacements to arrive at the office before you are back (ordering new hardware/server would increase recovery time should you not have a fast failover solution).

The importance of failback

Failback is the process of restoring your temporary failover solution to a permanent state, usually on the physical or virtual environment the system was before the disaster. In that time period it is important your failover solution continues to create backups to an accessible storage device.

Before shutting down the failover VM we recommend that you make a backup and use that to restore to the new server. You can easily do this via the Recovery process using ActiveImage Protector Recovery Environment, this ensures all changes that happened while you were using the failover VM are saved and are restored long term.



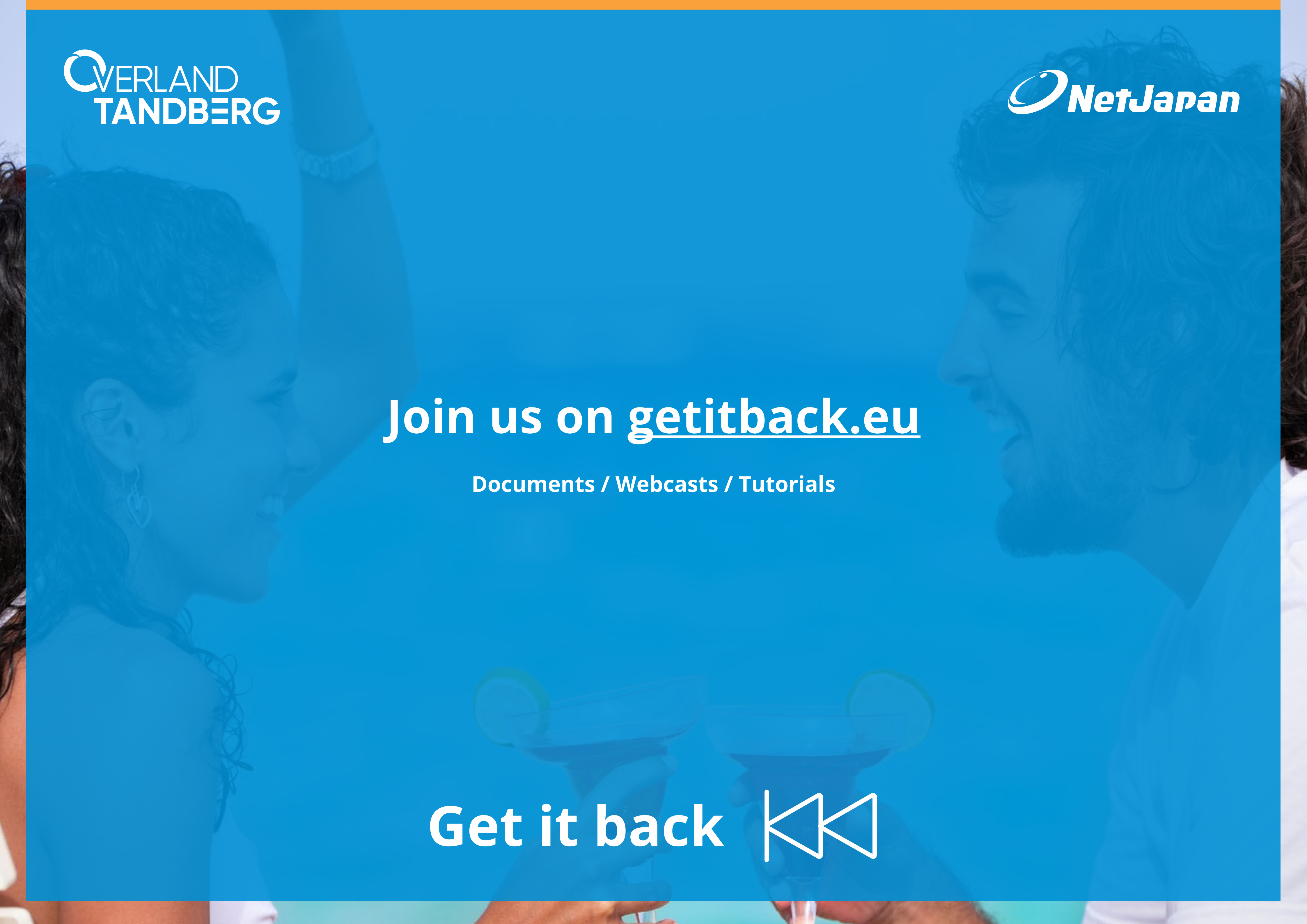
Conclusion

The summer holiday period is often stressful for IT Professionals and the increase of cyberattacks has forced us all not only to have protective security measures in place, but also to be able to rely on a flexible and secure backup solution that allows you to restore a previous state of your server as easily and fast.

Trusting your backup solution to do so is great, but controlling the situation is better!

By combining **Tandberg RDX QuikStor** or **QuikStation with NetJapan ActiveImage Protector** backup and disaster recovery solution, SMBs ensure a very high protection for their company and their backup files with the option to resume activity fast via remote in case a disaster happens.

To find out more how to combine and configure both solutions, check the following guides:
How to configure QuikStor with ActiveImage Protector
How to configure QuikStation with ActiveImage Protector (coming soon)



Join us on getitback.eu

Documents / Webcasts / Tutorials

Get it back