Ransomware
e-book

BEGIN

Disclaimer

The recommendations in this e-book and pdf should not be seen as something other than a guide. What we provide is an introduction to what one must consider when preparing to be able to handle an event such as a ransomware attack.

Our recommendations make up a small fraction of all the preparation that should be done.

However, if the recommendations are followed, you are on your way and stand a better chance of handling a ransomware attack than if you did not have these things in place.

AGREE AND CONTINUE

Table of contents

- Business Impact Analysis
- Key Recovery Target
- Recovery Point and Time Objectives
- Disaster Recovery Plan
- Backups
- Spare components
- Service Level Agreements
- Training

START JOURNEY

Business Impact Analysis

Everything starts with the BIA. As the name suggests, one must analyze the impact of a cyber attack on the business. This can be done in several ways, but the easiest might be to ask.

“What would it mean to us (the corporation) if the production stopped completely for a certain amount of time?”

In this case, we assume that the cause of the stopped production is a cyber security event, but it could be a fire, earthquake, or anything else.

It may be valuable to break the question down into chunks of time; what is the impact if we are down 1 hour, 8 hours, a few days, or a few weeks? One of the goals is to define a monetary amount for each example to have a measuring stick to which to compare cyber security investments. If the BIA is low, one shouldn’t spend much on cyber (unless under regulatory compliance). At the same time, if the BIA is enormous, one must set aside an appropriate budget for cyber security.

Take a moment and think about what a complete production stop would mean to your company.

NEXT PAGE

Key Recovery Target

Some production facilities have several (DCS) systems.
If you have multiple DCS systems, which are the most critical? Which ones must be operational first, and which can wait until later?

Remember that a critical system may not be critical only because of revenue. Factors like environmental or compliance (or any other reason) may sometimes be more critical and hence must be addressed first.

Refrain from assuming that the most prominent system is the most critical and do not consider everything equally important. Falling into either of these traps will lead to wasted effort and pain later.

In our example, simply consider your primary DCS system as the critical one that must be brought back up for you to operate.

NEXT PAGE

Recovery Point and Recovery Time Objectives

RTO < 1 hour
The system is critical, and no downtime is acceptable.

RTO < 8 hours
This is an important system that must be back quickly.
It is not easy to achieve an RTO of a few hours, but with the right mix of technology and process, it is doable.

RTO < 3 days
Most production (DCS) systems fall under an RTO of days. It is reasonably quick and completely manageable.

RTO < 5 weeks
This is not a critical system; it will get back once other items are addressed.

RTO > 5 weeks
Similar to RTO < 5 weeks with the added time to source new hardware.

RPO in hours
Essentially no data can be lost. For DCS systems this is not very common.

RPO in days
A few days of data can be lost without too much trouble.

RPO in weeks
Weeks of data can be lost. Backups are taken after changes are done to the system.

Production system with data is mirrored onto a hot spare system.

System image backup of the system frequently restored onto hot spare system.

DCS System backups
+
warm spare

DCS System backups
+
system image backups
+
cold spare

DCS System backups
+
cold spare

DCS System Backups

NEXT PAGE

Consider which RPO/RTO combination that best meets your BIA need. RTO essentially means the same as your maximum allowable production downtime.

Disaster recovery plan

By working out the BIA, RPO, and RTO, you have learned a lot and have a solid foundation.

You should now have a document with the results and justifications from your business impact analysis. You also should have a section outlining the recovery point and time objectives. If you have different RPO/RTO for different targets, you should have documented that too.

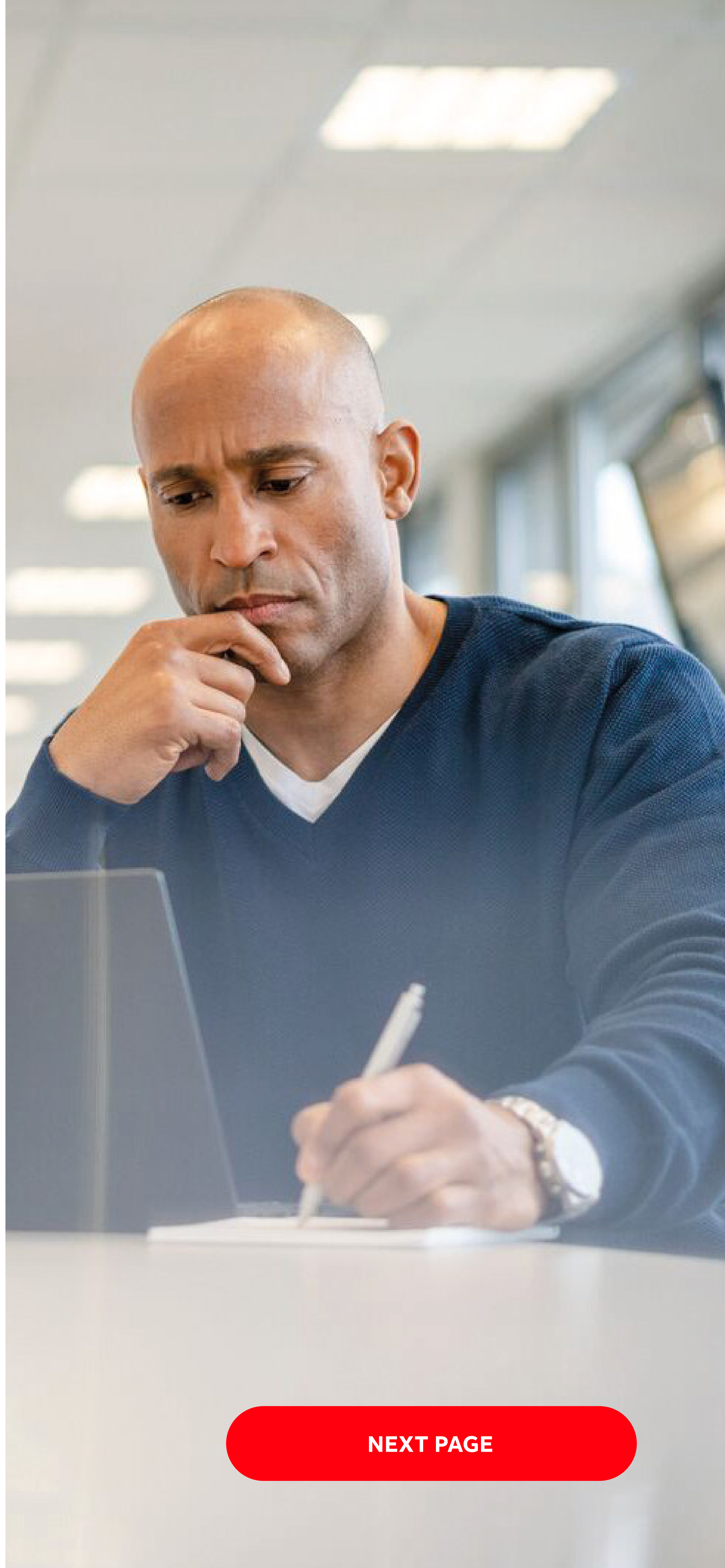
The next thing to document is a disaster recovery plan. This is not an easy task, nor will it be done quickly, but it is essential.

The plan should include everything and anything you can think of that would be needed during a crisis. Imagine that your whole DCS system is gone. What steps must you take to get from complete disaster to restored production?

Remember edge considerations such as a communication plan. This is who should talk to the press. Saying the wrong thing may worsen the situation regarding the stock market, customers' trust, and public opinion.

Another fundamental thing to document is a contact list, who to contact in the case of an emergency. Don't forget to have redundancy incase the first person can't be reached.

⚠ Do not think you don't need a DRP!



NEXT PAGE

Backups

When preparing for the worst, one must have solid backups of any computer device required to operate. If you fall victim to a ransomware attack and don't have a backup, you are forced to trust that the attackers will provide the decryption keys after you pay them, and even if they do, you cannot be sure that everything will be recoverable.

Backup type	What is backed up	Benefits	Drawbacks
DCS system backup	A backup of the control system's critical files. This backup can restore the system after the base system is manually restored.	Included in the DCS system.	Requires a fully configured system for restoration.
System image backups	These are complete backups of everything on a computer and can be used to restore the full functionality in the case of a crash.	One backup with everything needed for restoration.	Time-consuming and requires much storage. Specialized software.
Mirroring data	This is when data from the production system is almost instantly copied (mirrored) to the hot spare system. This makes it possible to achieve very low RPOs.	Instant restoration.	Complicated and expensive setup. Custom-made solution.

The RPO/RTO combination you selected defines which backup type you need

NEXT PAGE

These backups can be used in conjunction to achieve specific goals. For instance, a DCS system backup can be restored after a system image has been used. Maybe the system backup runs every hour, but the image is only taken monthly. This mix is often very advantageous, but every type and combination also has weaknesses.

Backup procedure

A backup procedure is simply a written instruction on how different backups must be configured to meet the set RPO/RTO.

Backup validation

It is not enough to take backups; one must always test or validate them to ensure they are working. One does not want to be in a situation where one must use a backup only to find out it doesn't work.

NEXT PAGE

Spare Components

To recover from a cyber attack such as a ransomware attack, one must restore the backups to working hardware. Naturally, one can use the old hardware, but this is not always a good idea as the attacker may have infected the sub-systems within the current hardware, or the infected hardware must be left for the forensic team.

In the cases below, one can see that it is only in the case of cold spares that one can even consider reusing the old hardware, as both hot and warm spares require separate hardware from what the production system uses.

Hot Spare

Hot Spare is a spare part, in our case a DCS system, that is ready to take over instantly (or very quickly) if the primary system fails. The only way to have a hot spare is to mirror everything from the production DCS system to an identical copy of that system.

This is extremely complicated and, in some cases, not technically or at least practically possible.

Warm Spare

Warm Spare is a spare part, in our case a DCS system, that is ready to take over quicky with a few actions if the primary system fails. In this case, the spare part system can be ready in hours.

Keeping a warm spare is complicated and resource intensive.

Cold Spare

Cold Spare is a spare part, in our case a DCS system, that is ready to take over after some configuration and setup if the primary system fails. In this case, the spare part system can be ready in a matter of days after the hardware is loaded with OS and DCS system data.

Keeping a cold spare is easy but must be maintained as any other equipment to ensure that it is working.

NEXT PAGE

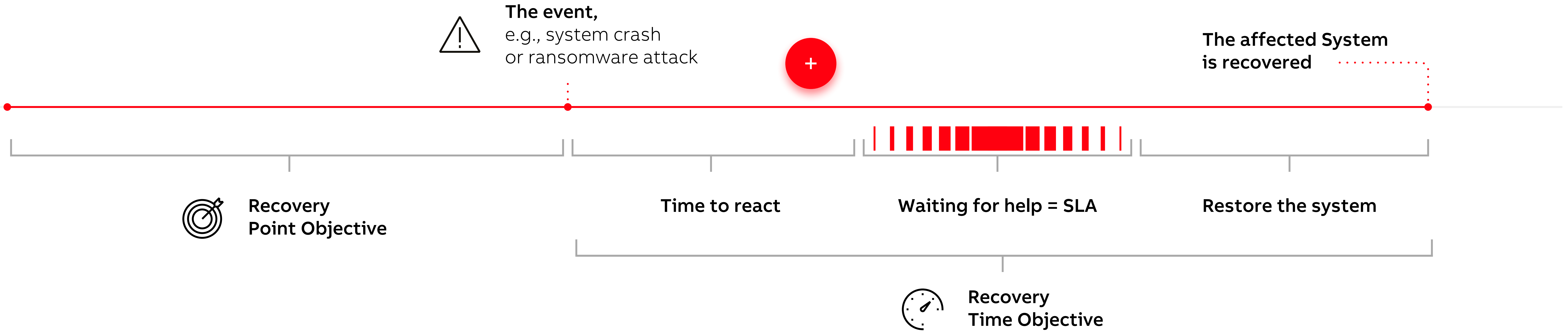
The RPO/RTO combination you selected defines which spare type you need

Service Level Agreements

Ensure that SLAs support the goal.

At this stage, you have a BIA that has helped you determine the RTO and RPO. Further, you have created and documented the plan, sourced and installed the backup software, and ensured that you have hardware ready for when you need it.
Now it is time to review and renegotiate your Service Level Agreements (SLA).

You want to ensure that the SLAs in place support the RTO. If the SLA for the 3rd party specialists, that you need to help you recover the DCS system, stipulates that they can show up after your RTO expires you may never be able to achieve your objectives.



NEXT PAGE

The SLAs in place to support your objectives can never be longer than RTO minus the time it takes to restore the system. For instance: You have an RTO of 24 hours. You know from your exercises that it takes 8-12 hours to restore the system after you start the work. This means that the 3rd party experts required for the restoration can have an SLA of up to 12 hours, but not longer. Don't forget to consider the initial time to react, which may be anywhere from a fraction of an hour to several hours.

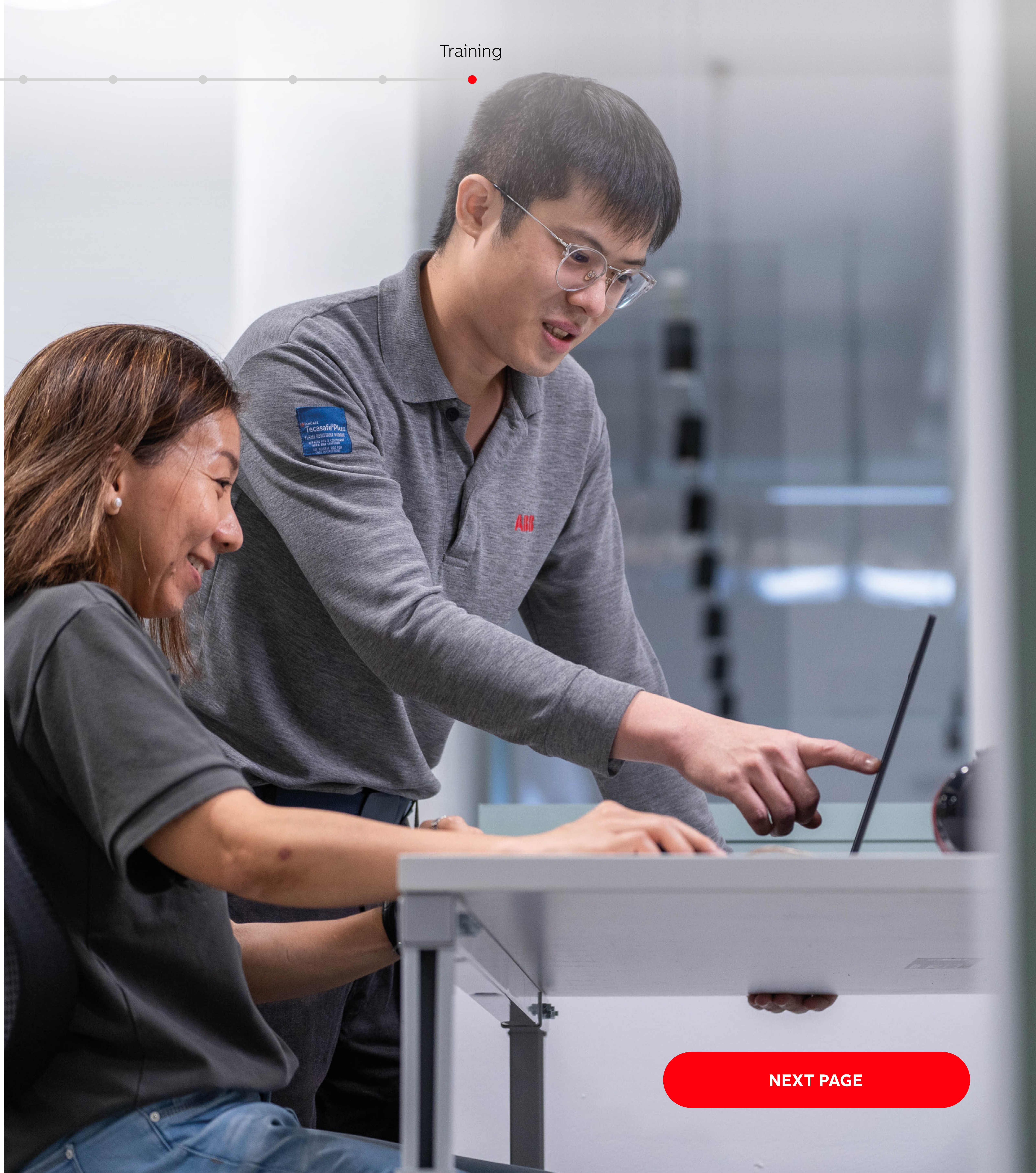
NEXT PAGE

Training

Now we have reached the last piece of the puzzle – training.

For a system restoration to be successful, one must conduct training and repeat it regularly. This is to verify the disaster recovery plan and your organization and partners' ability to achieve the RTO.

Different training methods range from tabletop exercises to full-blown live tests. Neither by itself is a good approach. One must balance the cost with the received benefit. Often a mix of the variants that exist between these two should be leveraged. Only performing tabletop exercises will not expose potential weaknesses in the plan, while a full-blown restoration is costly and disruptive.



NEXT PAGE

Wrap-up

Working through all the steps covered in this e-book will help you prepare for the worst-case scenario. Remember that what you have learned is only a start, and depending on the outcome of your business impact analysis, you may have to cover more steps and add more details to the ones covered here.

START OVER

FINISH

ABB