WESTPOLE

A matter of smart business and avoiding disasters

CYBER RESILIENCE

Index

INTRODUCTION

The prevalence of cyberattacks and costs of adverse cyber events such as data breaches, ransomware attacks, and accidental outages of critical IT systems have increased over the past few years.

As organizations have a more **complex and hybrid IT infrastructure**, data are leveraged across and beyond the company, digital has moved to the core of the business and **digital transformation** has become ubiquitous, the **importance** of **secure environments** is higher than ever before.

Traditional approaches to **cybersecurity**, **backup**, and **disaster recovery** are still **essential** to achieve availability, integrity, and continuity. Yet, depending on the organization in most cases, various protection mechanisms don't suffice anymore for reasons we cover in this whitepaper on cyber resilience.

CYBER RESILIENCE IN A NUTSHELL

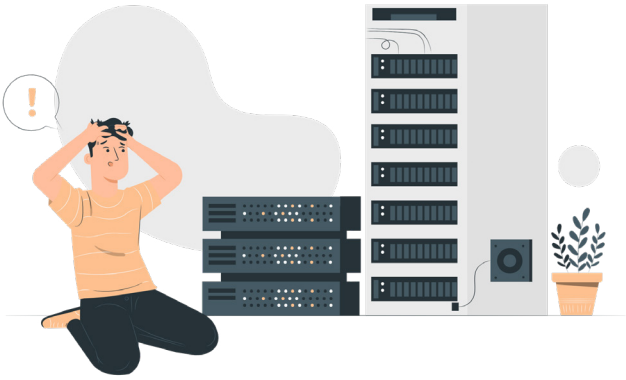
What is cyber resilience? And how is it different from cybersecurity? Each company knows the importance of cybersecurity and data protection. Everyone has invested in tools, processes, and strategies to prevent cyberattacks and mitigate the damage they do.

You might be **ready for cyberattacks** and **data breaches**, but are you also prepared to have your core IT systems, data, and digital business platforms function in case an attack affects you? And how resilient are you when **ransomware** has **encrypted all your data**, making them unavailable for the business? Are you even sure a **restore** will work and get you back on your feet?

Cyber resilience isn't just about **preventing** and dealing with cyberattacks and routinely performing cybersecurity tasks. It's first and foremost about an organization's ability to **continue to deliver** mission-critical services in the face of cyber incidents. In other words: it's about business, and that's also the perspective a good cyber resilience strategy starts with. Cyber resilience encompasses various functions and includes elements of business continuity, risk management, and disaster recovery, on top of cybersecurity. And it requires **regular testing**, for instance, to make sure a restore won't break your systems.

In these data-driven times where data, turned into actionable information, is a business asset and driver of value and innovation across all business functions, the increasing complexity of and reliance on the digital realm, requires such a holistic resilience approach that goes beyond cybersecurity.

The costs and indirect impact of data breaches and cyber incidents



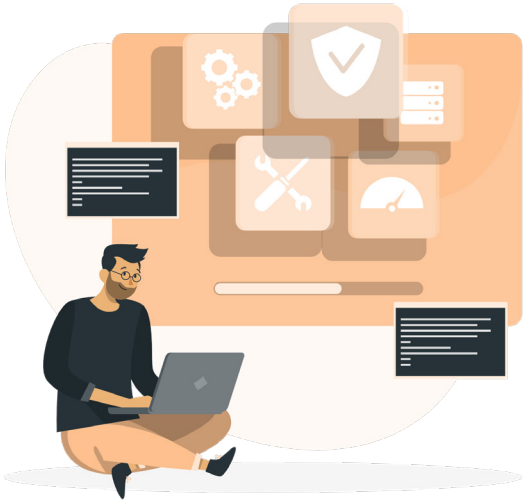
Customers and workers expect systems to be always on, breaches can lead to litigation and impact a brand's reputation, and cybercrime has become big business with ransomware as a perfect example of potential direct costs.

According to the 2019 Cost of a Data Breach Report by Ponemon Institute, sponsored by IBM Security, the average cost of a data breach reached $3.92 million, an increase of 12 percent over the past five years. And it's not just about large organizations. The report also found that the consequences of a data breach can be particularly acute for small and midsize businesses. Companies with less than 500 employees and typically earning $50 million or less in annual revenue, suffered losses of more than $2.5 million on average. Even if there are differences from a risk perspective, all industries nowadays are targets of cybercriminals. And so are all organizations, regardless of their size. No wonder that in 2018, the World Economic Forum, ranked cyberattacks third as most likely to occur and sixth in terms of likely impact in its Global Risks Perception survey.

Strengthening your cyber resilience means strengthening your capability to maintain mission-critical operations, rapidly recover your IT in the event of a cyberattack and minimize business impact. As a consequence, it requires a real understanding of the business, where and how data is leveraged, the different processes in the organization, and the applications, production environments and development environments.

Looking at backup and disaster recovery from such a holistic business – continuity – perspective inevitably has an impact on the way it's organized, planned, tested, and prioritized in terms of business decisions that might need to be taken once disaster hits.

No digital transformation without cyber resilience



It's clear that for organizations that are very far on a digital transformation journey and intensively use digital technologies across their business ecosystem, preparing a cyber resilience strategy does take time. Moreover, ample stakeholders need to be involved, given the fact that with cyber resilience, we're taking a risk-based approach.

Yet, even if your company relies less on IT for core business processes or doesn't have a complex hybrid IT environment, it's worth looking at cyber resilience, for instance, for regulatory reasons.

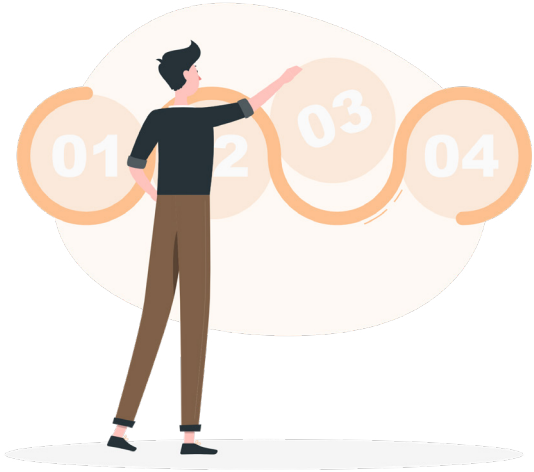
Organizations also accelerate their digital transformation in several areas. We've seen the impact of COVID-19 on our usage of digital platforms, and it seems inevitable that phenomena such as remote work to name one will be more broadly adopted, again adding to the risks.

Last but not least, as mentioned, all organizations are a target, and even if they aren't a direct target, they can become a victim of an attack.

Did you know that in the time it took you to read this, there have been several ransomware attacks across the globe since every 14 seconds one takes place? Researchers predict that by 2021 a company will be confronted with ransomware every 11 seconds.

Although there was a slowdown in the number of ransomware attacks as Bart Donné, General Manager at WESTPOLE Benelux explains in an interview on ransomware and Disaster Recovery as a Service, the numbers went up again.

An actionable five-staged cyber resilience lifecycle approach



In the first part of the whitepaper, we covered the importance of cyber resilient risk management, and disaster recovery as the costs of data breaches and the number of cyberattacks grow.

As promised in this second part, we look at a staged cyber resilience lifecycle approach and its different components.

When setting up a cybersecurity strategy with the necessary applications, backup, and recovery possibilities and defences to protect your business from attacks and data breaches, you no doubt have already gone through planning and protection stages.

Yet, cyber resilience is broader, and it starts from the prioritization of what's crucial for the business (data, systems, processes,...) and includes testing, continuous updating/learning, and post-incident recovery.

So, it also requires a more holistic and strategic approach that involves various stakeholders, thus also creating internal awareness since you follow a business- and risk-driven approach. That's one reason why such a cyber resilience lifecycle framework comes in handy.

Secondly, for most organizations, it's impossible to do everything alone and automating several tasks that are necessary to strengthen robustness and guarantee business continuity is inevitable. And last but not least, a comprehensive framework enables you to spot internal weaknesses and overcome existing limitations in your current approach.

A cyber resilience lifecycle framework and the place of DRaaS

Regarding ransomware and Disaster Recovery as a Service (DRaas), some things need to be considered, such as a lack of fixes, a single-line defence approach, and issues with user access control. These and other challenges can be identified and tackled using the model we describe below.

IBM, WESTPOLE Benelux is a Platinum IBM Business Partner, has developed a cyber resilience lifecycle framework that is based on the cybersecurity framework of NIST. It consists of five phases. Below is a description of each one with the various outcomes per stage, which include avoiding the weaknesses and overcoming other hurdles.

The fact that most organizations can't do everything themselves and this is such an all-encompassing area with many elements to take into account and potentially severe consequences if not done correctly is precisely why many organizations go for a DRaaS approach. For smaller businesses, it offers the benefits of an end-to-end approach at affordable costs, and larger organizations can quickly scale it as the number of servers, applications, and databases they have grows.

Moreover, DRaaS, by default, includes the capabilities you need in the context of cyber resilience as it differs from traditional on-site disaster recovery, enabling rapid post-incident recovery from within a separate environment. An overview of the five phases of IBM's cyber resilience lifecycle to make it more tangible.

STAGE 1: IDENTIFY
A matter of understanding and priorities

In the identification stage, we primarily identify the critical assets, looking at what we have and how we need to protect it.

The 'identify' phase is built around the premise that you will be compromised, which is what cyber resilience is about to begin with. In other words: we identify from the perspective of how you will recover from a breach.

This phase includes the automated classification of your systems and data, with prioritization of what data needs to be restored first. We also define where what data is backed up, which depends on the Recovery Time Objective (RTO) for specific types of data classes. Further, the recovery process plan gets defined (for instance, how often is a test needed), and we want to understand the 'normal' data profile, or how data is 'normally' used. This is essential since it enables you to know when a ransomware attack, which typically is a gradual process, is being prepared as we can see suspicious behaviour and usage patterns. Once the 'identify' phase is finalized and documented, the resulting plans should be tested to make sure that data can be covered, and nothing has been left out.

STAGE 2: PROTECT
Beyond the backup

The protect phase is about detecting vulnerabilities before they are exploited and having the protection in place in your infrastructure with the use of air-gapped data protection and immutable storage technologies.

'Protect' isn't just about a backup whereby you protect your data by copying it somewhere else, encrypting it, and providing an air-gap copy. It's also about the protection of the overall environment. This includes safeguards such as identity management and role-based access controls, setting up a regular maintenance cycle *(including, for instance, patching, as mentioned today often a weakness)*, and defining proper information protection processes.

A plan regarding awareness and training and decisions on the leverage of protective technology also are typical outcomes in this phase, which essentially concerns developing and implementing the right safeguards to ensure delivery of critical services.

STAGE 3: DETECT
Monitoring to identify cybersecurity events

In the detect phase, we aim to discover cybersecurity events in a timely way. This is done by using automated testing and verification of backed-up data with advances analytics, enabling to stop attacks and minimize downtime rapidly.

Detecting attacks and breaches is an ongoing task and certainly not an easy one. Monitoring data performance anomalies and setting up continuous detection processes is possible on the primary infrastructure, the backup infrastructure, and in a logical way, with different solutions that IBM and WESTPOLE offer, with the right mix depending on your scenario and needs. They help identify day to day activity in the primary and copy data areas. In the detect stage, we monitor the performance of revenue-producing data and the copying of revenue-producing data. We also understand the changes in data reduction results.

STAGE 4: RESPOND
Plan, communicate, isolate, shutdown and prepare recovery

Effectively responding to cybersecurity incidents, in particular cyber outbreaks, is our primary goal in the response phase.

The development and implementation of the right activities and actions to take when a cybersecurity incident is detected include multiple aspects such as response planning, communications, and mitigation of the event to minimize disruption. In case a breach effectively occurs, one of the main actions to take is disconnecting systems from networks to avoid that breaches impact more data systems and isolate and shutdown what requires doing so.

This also means that you need to have an air gap copy available or can disconnect your backup servers from your live network and start the recovery of your core business applications in another, ideally new, environment.

STAGE 5: RECOVER

Optimizing for the most efficient recovery time objective when cyberattacks occur

And that brings us to the final phase. The 'recover' phase concerns the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, per the definition of NIST.

In practice, it means that we create and test procedural plans to recovery for when a cyberattack or breach occurs, and data on primary revenue-producing systems is compromised. In other words: recovering access to the critical data and applications the business needs. The recovery phase focuses on recovery planning but also on improvements and, again, on communications, essential in times of adverse cyber events.

The previous phases in our cyber resilience lifecycle now all matter. While we identified the critical data to recover first, now we want to do so in practice, keeping in mind the most efficient RTO, the recovery time objective.

Cyber resilience solutions for each scenario and phase

As you can see, cyber resilience can be quite a daunting challenge indeed, with several considerations, plans, and actions to take.

Fortunately, a DRaaS solution helps you automate many functions and performs several of the mentioned tasks, also offering post-incident recovery thanks to the replication of physical or virtual servers to allow switchover.

However, as said, no organization is the same. That's why, with IBM, we offer a full portfolio of solutions that are typically important across different of the mentioned phases, enable an orchestrated approach, allow for the use of various (multi-cloud and on-premises environments) and support different storage means. Moreover, most solutions enable additional functionalities. Describing them all in a single blog would take us too far, so get in touch to talk about the cyber resilience solutions that fit your organization and plans best.
You can also read more about two of the solutions, IBM Spectrum Virtualize and IBM Spectrum Control, in our article on total storage. IBM Spectrum Virtualize is one of the key components of the overall offering and enables to virtualize the storage layer and give it additional capabilities such as compression, encryption, and performance monitoring, which can be passed on to other solutions.

Get in touch to learn about all the solutions and capabilities for your needs.

IBM Platinum Business Partner

More information about cyber resilience

CONTACT US

WESTPOLE