# THE DISASTER RECOVERY MATURITY FRAMEWORK


Apex
Technology Management, Inc.

Transforming Organizations and Lives
Through Innovative Technology Solutions

apex.com · (800) 310-2739 · info@apex.com

## Climbing The Recovery Maturity Curve

Apex Technology Management understands that businesses are critically reliant upon IT systems – which means you're facing significant financial harm when they go down. We know that you've probably worried about all the potential causes of downtime: lost or corrupted files, application failure due to a software virus, hardware malfunctions, power outages, or a natural disaster that can take out an entire facility.

For decades, IT managers have protected their infrastructures using a combination of preventive measures and recovery and restoration activities to bring IT systems back to normal operation as quickly as possible. As companies like yours continue to grow and update their IT infrastructure, different tactics are being employed to ensure the critical systems and applications are always accessible.

These tactics are strategically based on business needs, budget, size of the IT department, regulatory requirements, and more. Seldom will two companies in the same industry and of the same size have the same disaster recovery architecture, as it relates to technology, overall DR plans, and processes.

## The Cost of Downtime

Each year businesses in North America lose $26.5 billion due to IT downtime.

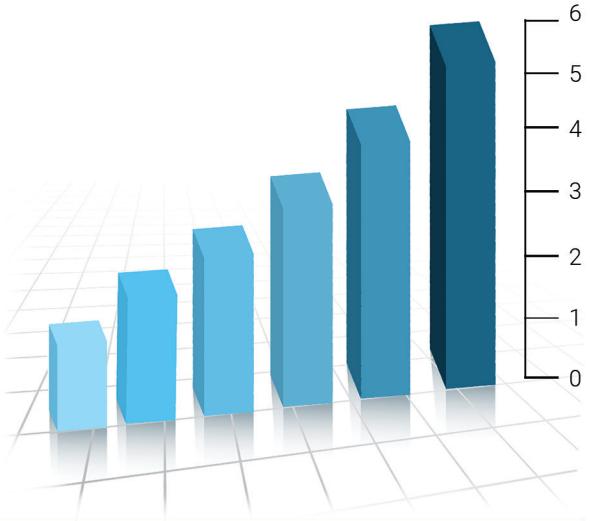
For small and medium-sized businesses with less than 1,000 employees, downtime is estimated at a minimum of $12,500 per day. These financial losses are attributable to multiple factors:

- **Inability to generate revenue while data or systems remain unavailable**
- **Falling out of compliance with contractual commitments or regulatory requirements**
- **Damage to the company reputation because IT systems were unavailable**
- **Customer defections due to brand damage**

Even worse, downtime can be fatal for a small business. A firm suffering a major data loss has a 70% likelihood of going under within a year; businesses that survive find it difficult, if not impossible, to regain the market share they previously enjoyed.

### FINANCIAL IMPACT BY COST CATEGORY

- $5,760,000: Reputation and brand damage
- $3,983,000: Lost productivity
- $3,183,000: Lost revenue
- $2,533,000: Technical support to restore systems
- $2,381,000: Cost of forensics to determine root cause
- $1,662,000: Compliance or regulatory failure

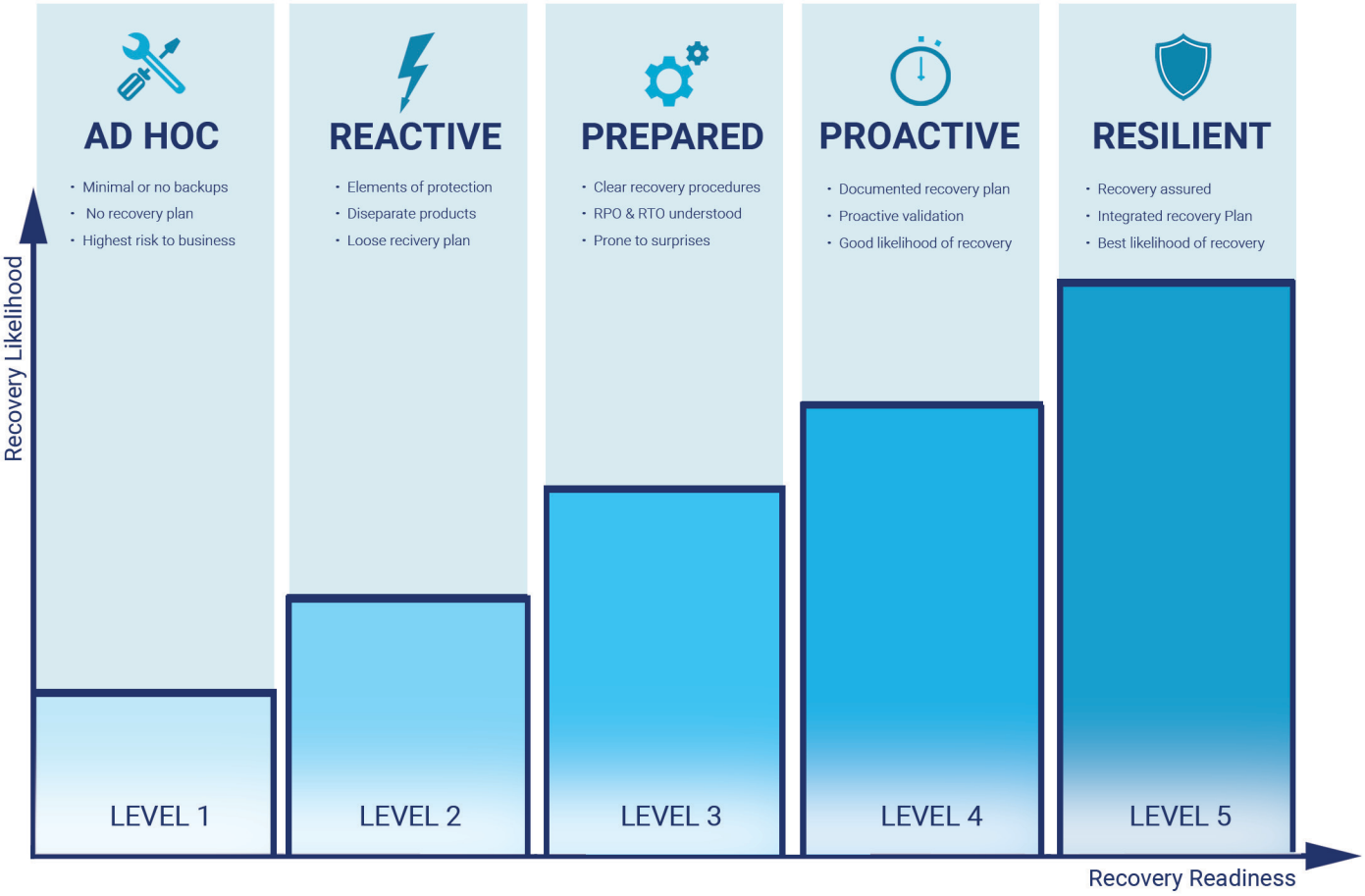



Source: IBM Global Study of the Economic Impact of IT Risk

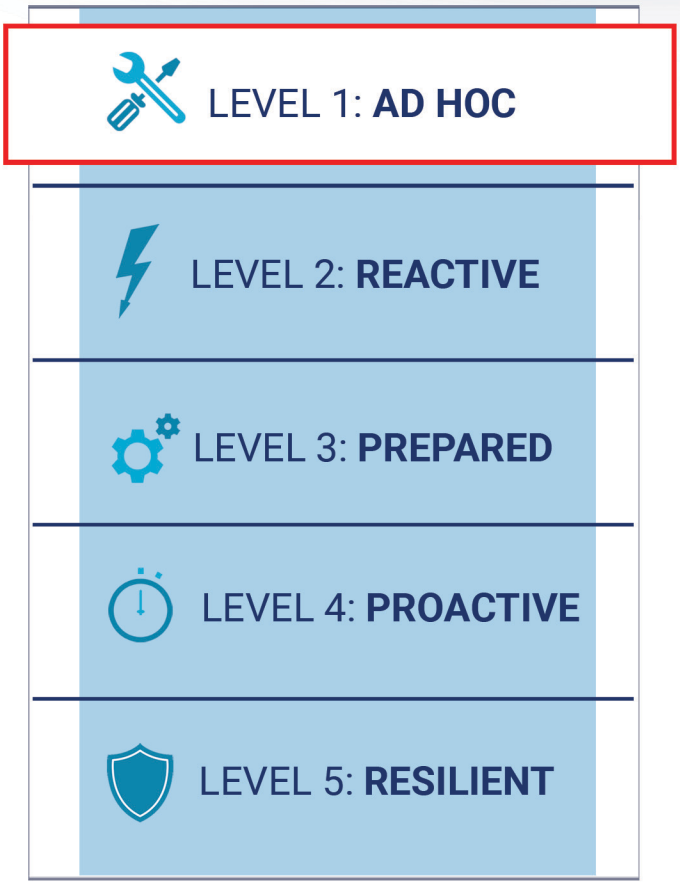
## Recovery Maturity Curve

To avoid these consequences, it's essential for your business to implement a plan that enables rapid recovery from application downtime. Each business has unique needs and tolerance for risk, which factors into how prepared an organization is for dealing with an unexpected outage. Astonishingly, 57% of small businesses don't have a disaster recovery plan in place and only 23% back up their critical data on a daily basis.

A company's state of recovery readiness can be illustrated by a maturity curve, as shown below.



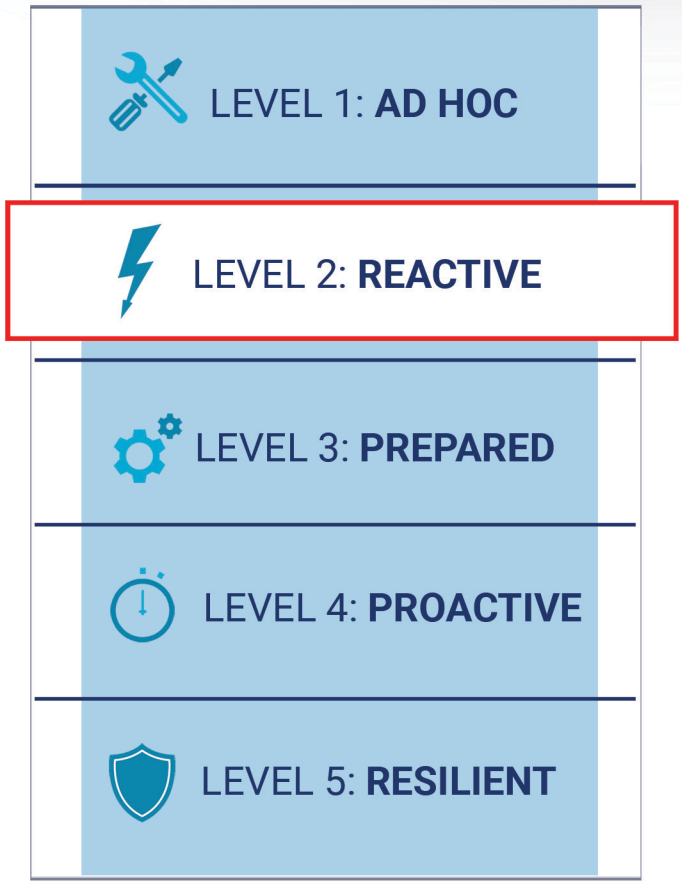
# LEVEL 1: **AD HOC**




In this case, almost nothing is being done to ensure readiness to recover from an outage. There may be occasional backups, but recovery is completely ad hoc. The absence of a recovery plan means any event causing downtime will trigger a scramble to try and figure out how to recover. This is how many organizations address the issue of IT recovery.

Even documenting a few critical technical and business recovery procedures would be a big help, but most organizations don't take the time for this. A key concern is that there may be little or no senior management support for such an activity, although senior managers will certainly have plenty of questions if their systems suddenly go down.

# LEVEL 2: **REACTIVE**

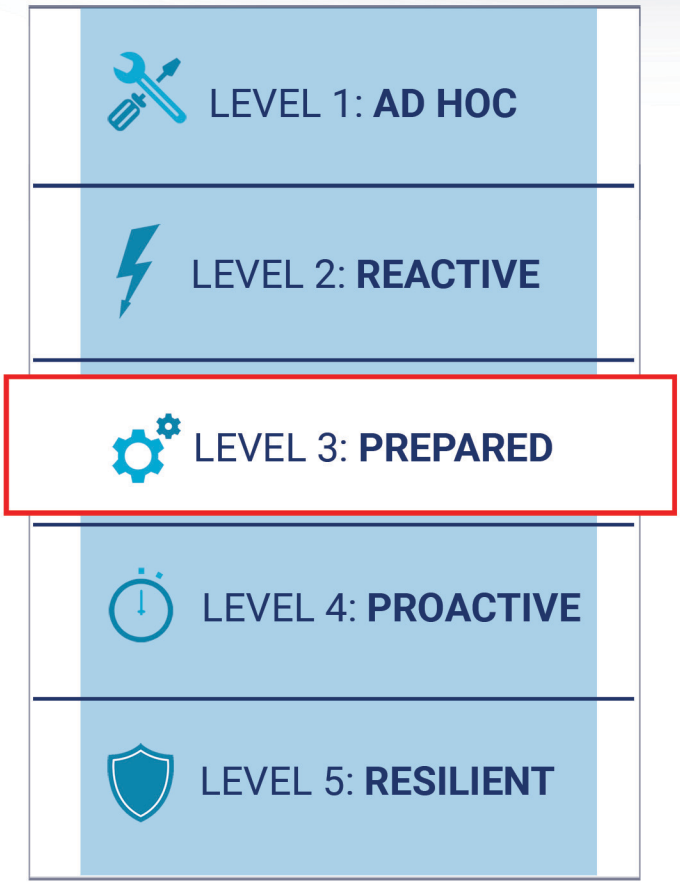



Elements of protection are in place, which may include scheduled local backups, remote copying of data for disaster recovery, and possibly server failover mechanisms for business continuity. These are usually implemented using disparate products that incur overhead charges that are expensive to deploy and manage.

Recovery planning consists of loosely sketched guidelines or is completely reactive, which decreases the likelihood of smooth recovery from an outage. Lack of documentation of emergency recovery procedures is also a big concern, and the simple act of writing down specific procedures is often a major step forward in improving the ability to recover.

A common example where Level 2 falls short is a corrupted application database for which a recent backup doesn't exist. After recovering an old version of the database, productivity suffers as the database is manually repopulated from paper records or other data sources. Another example is the need to save money on the department budget, so the acquisition of certain systems, such as backup power or a backup server, may be deferred or not pursued.

# LEVEL 3: **PREPARED**

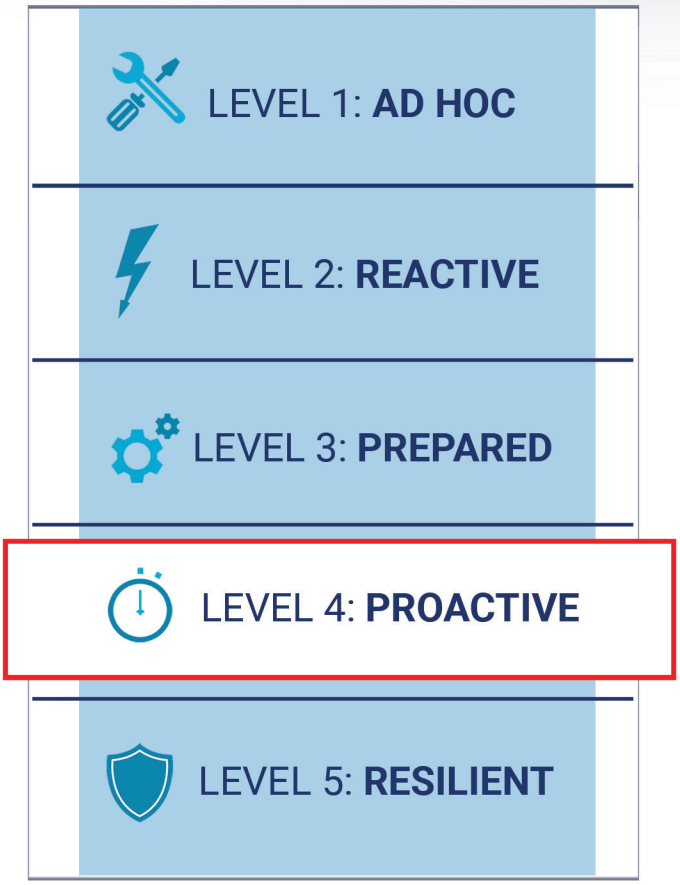



The organization is prepared with a documented plan with clear recovery procedures. The plan is aligned with business needs in terms of recovery point and recovery time objectives (RPO and RTO). However, last minute heroics may be necessary to deal with surprises during a recovery operation.

A real life example where Level 3 had an unexpected wrinkle was with a business that dutifully backed up its server images to the cloud, as specified in its disaster recovery plan. However, due to an oversight in execution, a backup wasn't updated when one of the servers had been replaced. As a result, when Superstorm Sandy hit and the customer needed to virtualize its servers in the cloud, one server was incompatible with the others, resulting in on-the-fly attempts to solve the problem.

Another example emphasizes the need for periodic exercising of DR plans. An IT department was confident it had the skills and resources to recover a critical server. However, the exercise showed that changes in the server's configuration had been made, but the recovery plan had not been updated to reflect those changes. Naturally, the exercise was a failure.

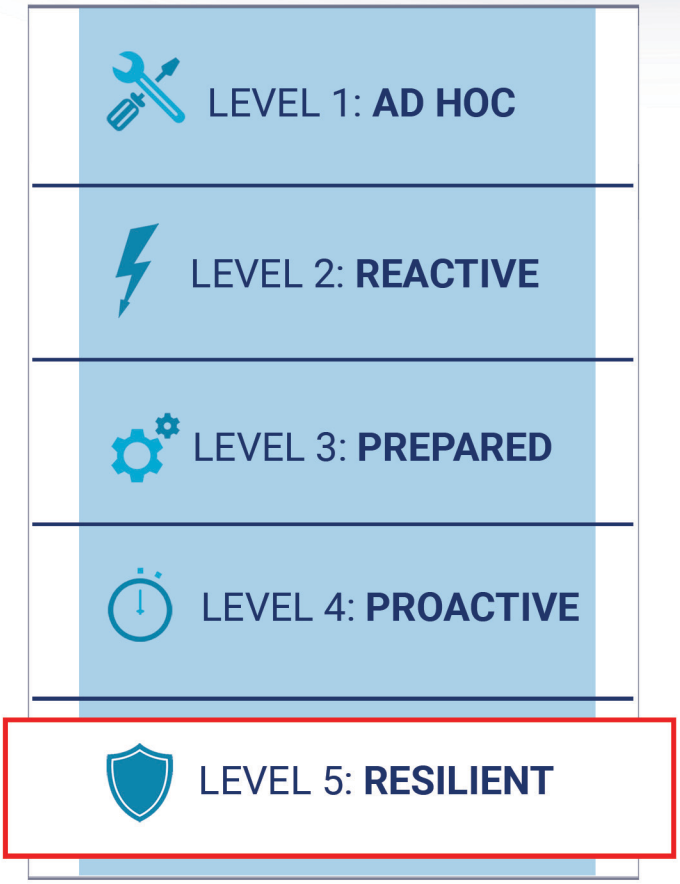
# LEVEL 4: **PROACTIVE**




A recovery plan exists, as described in Level 3. In addition, proactive validation of the plan is performed by testing local recovery procedures and performing periodic disaster drills. Routinely exercising the recovery plan drastically minimizes the risk of missing an RTO.

As emphasized in DR standards and good DR practice, DR plans and its associated elements are "living" documents that must be periodically reviewed and re-validated to ensure that the plans are consistent with the company's business objectives. Additionally, by reviewing and re-validating DR plans, businesses can provide assurance that they will be ready to use and accurately reflect the true state of the systems to be recovered.

# LEVEL 5: **RESILIENT**




A detailed recovery plan exists, it is fully integrated with business continuity plans that are also in place, and there is a fully organized disaster recovery program to provide administrative oversight on all activities associated with disaster recovery. Preventive measures to minimize the potential for threats have been established. Senior management of the organization fully endorses the importance of technology disaster recovery planning, and senior managers periodically attend plan exercises as observers.

The organization has been able to achieve a state of resilience using a balanced configuration of resources that include on-site hardware and software, virtualized systems and storage, and either an advanced third-party managed services provider or a cloud-based disaster recovery provider. The organization is confident that virtually any incident can be addressed quickly, with minimal damage, and IT systems and business processes can be returned to normal production well within RTO and RPO limits.

## Looking Deeper

The maturity levels described speak to the overall state of readiness to recover from application downtime, whether due to loss of a single file, complete outage of a data center, or anything in between. Apex Technology Management can help you gain a better understanding of recovery readiness by assessing a number of key factors:

- **Impact of Application Downtime:** How severely would application downtime impact your business? At what point in time would you business begin to suffer without the availability of critical systems, databases, and customer data or network resources? Beyond what point in time would you business be irreparably damaged following an extensive loss of IT resources?

- **Recovery Time Objective (RTO):** How much downtime can you business withstand? Is it minutes, hours, or days? RTOs must be identified for all mission-critical systems, networks, databases, and other IT resources. They are a key metric when preparing DR plans.

- **Recovery Point Objective (RPO):** This metric represents the amount of time data can "age" before it is no longer useful to the company. The shorter an RPO, the more critical the data. Your backup process must be robust enough to replicate data in the shortest amount of time between the original and replicated copies.

- **Protection Architecture:** Does your protection solution provide local recovery, cloud recovery, or both? Is your solution built from one or multiple products? Does your network infrastructure have sufficient resilience to support the protection architecture with diversely run circuits and sufficient bandwidth to handle normal and emergency traffic demands? Is your protection architecture scalable enough to support an out-of-normal situation where more resources are needed than are available?

- **Protection Scope:** Which IT assets are being protected? User files, databases, core applications, server images, IT infrastructure? Will all elements of your IT environment be available and operational during a disaster in a way that allows employees to securely connect and continue working?

- **Documentation:** Are recovery procedures fully documented and up to date? Are multiple copies of procedures available in hard copy and electronic versions? Will emergency teams have access to copies of plans in their cars or in their homes? Will collaborative resources be available to securely store copies of plans? Will emergency teams have copies of DR plans on their smart phones? Will they be able to remotely access their plans using their smartphones?

- **Testing Scope:** Tests can be as simple as a tabletop walk-through of a plan. However, the amount of coverage when testing and validating recovery procedures is important. For example, are files simply spot-checked, are servers failed over, or is secondary infrastructure verified? These tests are also important to ensure that non-technical issues such as evacuation plans can be addressed, and that necessary financial arrangements and office supplies for a new workspace can be ready when needed. More rigorous recovery testing of critical systems, data storage and networks is needed to ensure these critical assets can be recovered and returned to production status quickly.

- **Testing Frequency:** How often are recovery procedures exercised? Experience has shown that a minimum of one test annually is a starting point for most IT systems, but for systems deemed mission-critical, it is advisable to test more frequently, especially if the critical systems have gone through a number of changes. DR plans need to reflect those changes, and this is where many plans fail: not keeping DR plans up to date with system changes.

- **Organizational Sponsorship:** Is recovery readiness an IT project or a company-wide initiative? Does senior management of the company, and not just IT management, support the need for disaster recovery? Has management approved a budget for DR? Has the IT staff received training in DR procedures from equipment vendors and network service providers?

Achieving Level 3 (Prepared) is an ideal initial goal for most organizations because it demonstrates an awareness of and commitment to key DR metrics, including RTO/RPO, documentation, testing and sponsorship. Aiming for Level 4 (Proactive) can be achieved by working with Apex Technology Management to leverage the unique benefits of cloud-based solutions.

## Is the difference between Level 3 and Level 4 worth the potential investment?

Apex Technology Management works with you to make that investment worth while. With a DR plan aligned uniquely with your needs, you maximize your budget and gain peace of mind knowing that your security is accounted for. Recovering your IT systems quickly using managed DR services ensures that you can return to "business as usual" quickly and are therefore more likely to reduce the financial and reputational losses your organization could sustain with a prolonged loss of IT resources.

Moreover, if your disaster recovery strategy anticipates situations that may become threats and initiates measures to shield your organization, you can advance toward Level 5, a fully resilient infrastructure.

The process of recovering IT resources following a disruptive event has traditionally taken many forms, mostly based on physical solutions such as backing up data, databases and systems to on-premise tape or disk systems; backing up the same resources to off-site data storage facilities; or data replication using mirroring techniques to managed data recovery services.

It is this last option – managed recovery – that provides significant promise to organizations of all sizes.

Recent developments in technology have made DR much more affordable, intuitive and available to companies almost anywhere. The emergence of cloud-based data backup and disaster recovery services provides new opportunities for IT departments to move up on the maturity curve. Users running traditional backup and recovery solutions may never rise above Level 2 maturity. Using managed services can speed up an organization's maturity simply by leveraging the resources of our team.

## Improving Readiness with Recovery-as-a-Service (RaaS)

The historical impediment to climbing the recovery curve has been affordability. In other words, because traditional software and hardware solutions tend to be too costly to deploy and maintain, businesses are forced to accept the risk of potentially dire consequences due to an IT outage. Additional reasons for the inability to climb the recovery curve include the lack of management support, lack of sufficiently trained staff and a perceived lack of need.

With the emergence of Recovery-as-a-Service (RaaS), your business no longer needs to settle for risky recovery practices. RaaS offers enterprise-class recovery-as-a-cloud service at a price point that's acceptable to even the smallest of businesses. This affords you the opportunity to cost-effectively move up the Recovery Maturity Curve. RaaS not only offers a proven solution for businesses, but also an opportunity for service providers like Apex Technology Management to layer our best practices on top and deliver cloud -based recovery to our clients.

## What really happens in a RaaS environment?

- First is the creation of a complete mirror image of the IT system you wish to protect. You can specify all or part of your IT environment, and there's no distinction between physical or virtual environments.
- Once images of all the IT systems you want backed up and ready for recovery have been created, you are ready to initiate recovery of those IT elements using a very simple Web-based process.
- Assuming the images created on the RaaS platform are current — and you can specify the level of RPO/RTO you wish for each IT element — you can access the most current version of the systems and data you need to recover.

The loss of critical systems and data — and potentially the loss of business — is minimized because you can access literally an exact image of the production environment you were using when the incident occurred.

Launching the transition from production to recovery environments is a very simple and secure process, much less cumbersome and complicated than traditional methods. RaaS gathers all the commands you need for a smooth failover and automates them so you can launch recovery from a smartphone, if necessary.

**Are you ready to finally gain peace of mind knowing that out-of -your control disasters won't cripple your operations?**

**Reach out to Apex Technology Management to speak with our team about the most effective disaster recovery plan for your unique needs.**

**Reach out to our team of experts at info@apex.com or (800) 310-2739 to get started.**