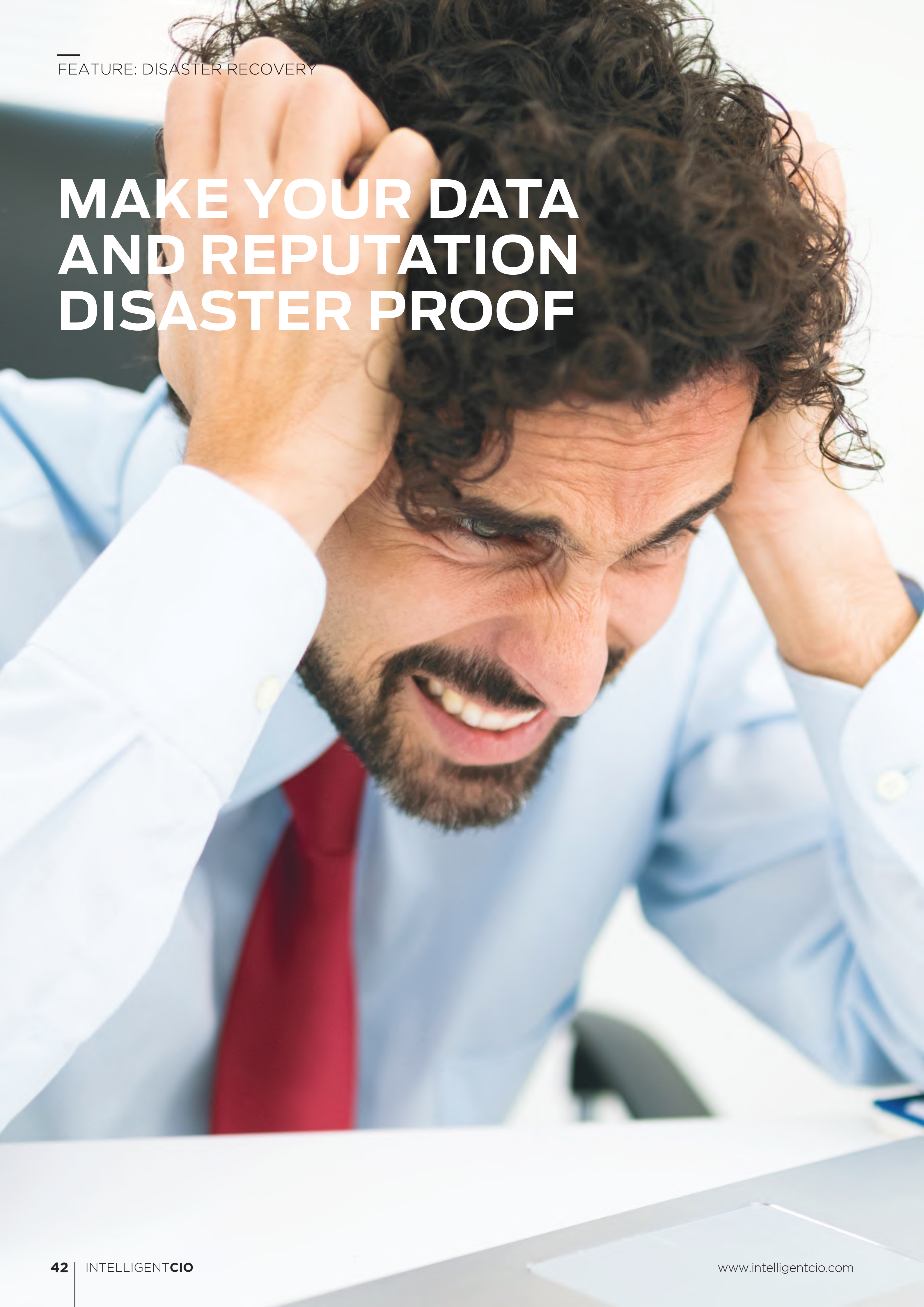
MAKE YOUR DATA AND REPUTATION DISASTER PROOF



Disaster Recovery is more vital than ever. The loss of data has more serious consequences than ever before not only because of the loss of vitally important information but also because of the cost of reputational damage that can have a major impact on business. In fact, it is no exaggeration to say that an effective Disaster Recovery system is absolutely crucial to the success of a business.

Imagine the ultimate IT disaster. A business loses its critical data following a natural or human-induced catastrophe. Loss of data can be caused by natural disasters such as floods, hurricanes, tornadoes or earthquakes.

But there are also man-made disasters to take into account such as hazardous material spills, infrastructure failure, bio-terrorism, and disastrous IT bugs. While it is not possible to prevent these it is possible to plan for such eventualities.

There is no doubt that if such situations are handled badly a company can suffer serious reputational damage which will do some sizable harm to the bottom line. In the worst cases, businesses can be put in a situation from which they can never truly recover.

Fortunately, in recent years huge strides have been made in effective cloud-based Disaster Recovery systems.

eHosting DataFort offers Disaster Recovery and Business Continuity solutions to recover business-critical applications in case of a disaster. *Intelligent CIO* spoke to Sachin Bhardwaj, its director of marketing and business development, about how to best prepare for the worst.

If disaster strikes and a company loses its data, what impact can this have on it?

94% of companies suffering from a catastrophic data loss do not survive – 43% never reopen and 51% close within two years, according to the University of Texas. Also, Gartner reports that seven out of 10 small firms that experience a major data loss go out of business within a year.

Data is crucial to businesses and the reliance on it is important not just for the current operations, but also for future growth. Since a disaster can strike in any form at any time, it can have very serious consequences on an organisation. It takes its toll at different levels, be it financial, reputation or confidentiality.

Given that most businesses rely on the use of technology for their operations, manufacturing, processing, sales and marketing, and with most departments relying on shared data, any loss of data can elevate and escalate the negative cost implications across the business. This can have both short term and long-term consequences. It is of even more consequence at a time when the news is spread rapidly across social media outlets and can have a crippling effect.

What is also important is that some data is confidential and can be connected to employees, customers, etc. While not only breaching the trust of the concerned people, it can also lead to huge amounts being spent on facing legal battles. And most of all, every organisation spends tremendous time and money to build customer loyalty and it is extremely difficult to regain trust should a company be faced with data loss.

"94% of companies suffering from a catastrophic data loss do not survive."

What are the main ways a company can find itself losing its data?

There are several reasons for data loss and they come in the form of human error, natural disasters, cyber-attacks, power loss, and malfunctioning of hardware or software.

- Cyber Attacks: According to a recent report by Gemalto, for the first half of the year 2016, 974 publicly disclosed data breaches took place in the first half of 2016, which led to the successful theft or loss of 554 million data records.
- Hardware or System Malfunctions: According to a survey of data loss's causes, more than two-fifth of users lose data because of hardware or system malfunctions. It is the most common cause of data loss.
- Human errors: Another common cause for data loss manifests itself in the form of clicking on the delete or format unintentionally or even the damage caused by physical damage by dropping the device.
- Computer Viruses and Malware: The risks involved in damage and loss of information at the current moment is also very high with the increasing number of virus, malware and ransomware attacks. This is applicable not just in larger enterprises, but also in smaller organisations. This can spread rapidly while causing temporary or complete damage to the business data.
- Natural Disasters: One of the most uncontrollable causes of data loss include earthquakes, fires, floods, etc. However according to a survey, natural disasters account for only 3% of data loss.

Sachin Bhardwaj, director of marketing and business development for eHosting DataFort

What is the best way to plan for Disaster Recovery?

A Disaster Recovery plan is a tabulated, organised and methodical approach with detailed instructions and preconceived responses to mediate accidental and unexpected disruptions. It is a comprehensive plan that includes anticipatory precautions, refined and scenario based reactions, reserve resources and redundancies so that the impact of a disaster can be contained and the enterprise can sustain essential operations as well as resume critical functions rapidly and with relative ease.

A few steps to get started:

1. Conduct a data assessment to better prioritise what data you need to have on hand after a disaster and who will need to have access to it.
2. Define an acceptable recovery time objective, recovery point objective and choose the right storage media.
3. Create a Disaster Recovery plan and test it.
4. Make sure sensitive data is properly encrypted.
5. Regularly back-up and snapshot data.
6. Make sure critical applications are always accessible.
7. Don't neglect laptops as according to Gartner, two-thirds of corporate data lives outside the data centre.
8. Maintain three copies of the data, stored on two different kinds of media, with one of them stored offsite.
9. Keep backups off site, in a safe location.
10. Store data in a secure cloud.

"Seven out of 10 small firms that experience a major data loss go out of business within a year."

We also suggest working with a trusted services provider to disaster proof data and IT systems. This will not only ensure high availability of the data and IT infrastructure, but will also let organisations focus on core activities that require their attention the most.

What does a Managed Disaster Recovery Service Programme cover?

A managed disaster recovery service will cover the following:

- RPO and RTO Service Level Agreements.
- Running a Disaster Recovery (DR) runbook for bringing up the DR environment.
- Making sure all systems and applications are up and running.
- Conducting frequent DR drills and rectifying issues that may arise.
- Liaising with vendors for support of various technologies in place.

“It is important that you continuously update your DR plan and test it by regularly running through different scenarios with your team.”

Earlier this year Commvault launched its new VM (Virtual Machine) Backup and Recovery trial software for customers and partners.

The software from Commvault, a global leader in enterprise backup, recovery, archive and the cloud, has significant enhancements on user experience, disaster recovery and cloud on-ramp.

Commvault’s VM Backup and Recovery software expands the company’s leadership in enabling customers to build, protect and optimise VMs throughout their lifecycle and migrate data and VMs to the public cloud of their choice, including AWS, Microsoft Azure and VMware.

Available as a free download to customers directly on the Commvault website, the VM Backup and Recovery software provides users the full experience of Commvault’s best-in-class software to back up and recover virtual machines, structured and unstructured data, as well as physical machines with speed and enterprise scale.

Commvault’s VM Backup and Recovery software is also available for partners to download on Commvault’s recently launched Partner Demand Centre, the company’s easy-to-use channel marketing automation platform exclusively designed for its partner ecosystem.

Intelligent CIO spoke to Nigel Tozer, the company’s solutions marketing director, about planning for disaster.

What is the best way to plan for Disaster Recovery?

It’s human nature to avoid addressing worst case scenarios unless you absolutely have to. But if you’re running a business in today’s technological landscape it is important to proactively develop and implement a Disaster Recovery strategy before catastrophe strikes. If you’re not available, you can be sure your competitors are.

Best practice Disaster Recovery plans include off-site data recovery at a second location, or provided by a trusted partner, a dedicated Disaster Recovery team, and a comprehensive recovery plan for employees to follow. It’s also important to have a third-party contact list of supplier specialists who can support your team during a crisis. Finally, it is important that you continuously update your Disaster Recovery plan and test it by regularly running through different scenarios with your team.

Nigel Tozer, solutions marketing director, Commvault

Tell us about the Disaster Recovery system(s) you offer.

Commvault offers a comprehensive, infrastructure neutral Disaster Recovery solution, that gives you maximum flexibility for your Disaster Recovery plans. Commvault software will backup your VMs, applications, data and endpoints with maximum efficiency based on flexible, automated policies, and enable you to recover your data rapidly and easily to meet your required service levels. Automated Disaster Recovery testing ensures you are always ready and confident, with comprehensive reporting to keep you informed and to drive continuous improvement.

Commvault software provides a single platform that has the broadest coverage in the industry, to protect and manage data and workloads for physical systems, VMs and cloud. Commvault has been named an industry leader in the Gartner Magic Quadrant for Enterprise Backup Software and Integrated Appliances for seven years in a row.

Do you offer tech support as part of a Disaster Recovery programme?

Commvault Customer Support delivers a range of world-class offerings that enable our customers to make significant efficiency savings and mitigate business and compliance risks. Every day their experience is helping our customers to implement DR plans that ensure consistent and reliable access to critical business applications and information.

Our comprehensive approach to customer support allows us to partner with customers to help them modernise their approach to IT and solve complex data growth challenges, while aligning with their key business and IT needs.

Veeam's expertise in Disaster Recovery has been recognised by the by Gartner Magic Quadrant for its data centre backup and recovery. This is the company's fifth successive year of being included in the report.

Intelligent CIO spoke to Rick Vanover, the company's director of technical product marketing and evangelism, about Veeam's approach to Disaster Recovery.

Could you start by outlining your company's expertise/offerings within the realm of Disaster Recovery?

At Veeam, we have put Availability as our top-line message. When it comes to disaster management, Availability becomes a critical capability that IT decision makers want immediately.

Our expertise is based on 10 years of undeniable innovation in the backup space, which paved the way for new capabilities that were brought to the market first by Veeam to transition to an Availability experience that has been enjoyed by over 230,000 plus organisations worldwide. This is going to be taken to a new level with our new Veeam Availability Orchestrator product, which will be available this year.

What would you identify as the different elements that form an

> **"I'd hope that organisations have given disaster recovery the requisite investment and preparation; but in fact this is not the case."**

Rick Vanover, Veeam's director of technical product marketing and evangelism, at Veeam

> **"The good news is that the technologies are available today to get organisations where their internal and external stakeholders expect them to be."**

effective disaster management strategy?

The strategy is very important. In fact, these are principles taken into account for the new Veeam Availability Orchestrator product, as well as options for organisations to build Disaster Recovery plans with Veeam today.

I'll share a few specific elements that can highlight this process. The first technology service needed in a disaster is communication.

Whether it is email or phone systems; communication lines have to be established. But the big indicator is that it's not just a mail server or phone system online; users and client software may need to be in place and pre-requisite systems may need to be online as well (such as DNS).

Additionally, a Disaster Recovery Management Strategy should be built in terms of applications and their associated requirements. This way, the business can decide and be made available in terms that they understand.

How have the associated technologies and strategies around disaster recovery evolved over the last few years?

The last few years have actually shown us that a Disaster Recovery strategy is very critical for organisations today. Specifically, there is no 'manual mode' for many businesses today. Just take the latest headline outage as an indicator of the dependency that data centres have in running any modern business.

That need for Disaster Recovery has evolved and technologies have paved the way for innovation – and Veeam is investing in this area significantly.

The key drivers and innovation areas that have enabled more advanced Disaster Recovery are advances in virtualisation technologies, cloud and service provider technologies and advanced storage systems. These infrastructure technologies pave the way for software vendors like Veeam to deliver a rich availability experience to organisations of all types.

To what extent would you say enterprises have become aware about the importance of Disaster Recovery, and to what degree have organisations taken the right steps to prepare themselves?

I'd hope that organisations have given Disaster Recovery the requisite investment and preparation; but in fact this is not the case. Each year, Veeam commissions the 'Veeam Availability Report' that surveys CIOs around the world and it's clear that there is always improvement needed in this area for organisations today.

The good news is that the technologies are available today to get organisations where their internal and external stakeholders expect them to be.

To prepare, I advise organisations to identify what applications and parts of the IT organisation are in-need of requiring a complete Disaster Recovery plan. Then apply the technologies to get there, test it accordingly and diligently ensure the documentation is updated. These are some of the principles that will be incorporated into Veeam Availability Orchestrator, and we see organisations of all types interested in delivering a complete Disaster Recovery plan for critical applications. ■