eGuide

FROM IDG

CIO COMPUTERWORLD CSO InfoWorld NETWORKWORLD

VEEAM

presents

Availability in the Age of the Cloud

Data is the lifeblood of most businesses, and it's everybody's job to protect it. On the other hand, it's IT's job to know how to protect it. In this age of the cloud, how safe are your mission-critical functions? Do you have a disaster recovery plan? How often do you revisit that plan? How often is it updated? Does everyone know what to do in the event of an emergency? We don't want to scare you, but this eGuide will help you to answer some of these questions.

Exploring the paradigm shift from backup to data protection

Smart organizations evaluate their overall data footprint and transform their traditional back-office IT to a streamlined data protection approach for both cloud and on-premises data.

BY GREG ARNETTE | Since the inception of computers and beginning as early as the 19th century, there has been a need to back up data in case of possible disasters, both natural and manmade, or hardware and software malfunctions. As computers have evolved over the years, backup technologies, philosophies, and processes have changed in parallel. For today's computing environments, backup is only one part of a comprehensive data protection plan for critical organizational, customer, and partner data. Even with hardware more reliable than ever before, there is still a critical need for a thoughtful, multi-faceted data protection plan.

The IT decision maker of 2018 is faced with several challenges and many opportunities. There are more technologies and services available than ever before to organizations—a veritable Sears catalog of affordable SaaS services. Organizations are going to continue to move more data to the cloud with an eye to the cost savings achieved by renting infrastructure as opposed to buying it and building it from the ground up. This also grants employees access to data everywhere, on any device with an internet connection. The increased complexity means that some data resides in the cloud, though most still remains on premises. That's why a sensible and well-thought-out data protection plan is a must.

Yesterday's back office and the rise of the cloud

With the rise of cloud and software-as-a-service (SaaS) displacing on-premises enterprise applications, some might think backing up the data is not a requirement: that's the responsibility of the cloud or SaaS provider, isn't it? This mentality is a mistake, as protecting cloud-hosted data should be a critical piece when implanting and reviewing data protection services.

It is true that the various SaaS providers—from Salesforce, Office 365, and Workday to the three thousand others—most certainly back up the data. And cloud providers also have some security advantages. For example, they offer many more contingency plans than a typical IT department does, with more diligence paid

Bringing organizational data to the cloud does not mean you leave access governance and security in the hands of the cloud providers.

to software updates and the latest technologies for malware detection, signature-based or other. It's worth noting that SaaS providers most likely offer more physical security for their data centers as well. However, at this level, this type of backup does not protect your organization from human error or malicious attack.

Essentially, bringing organizational data to the cloud does not mean you leave access governance and security in the hands of the cloud providers. In many cases, access and security controls, as well as usage tracking capabilities, are limiting.

Protecting data in the cloud is partly your responsibility

AI-powered malicious bots from the "dark web" can assume user behavior patterns and ruin data stored in SaaS services. Granted, these black-hat bots can also do harm to on-premises systems, and this is why the IT department down the hall has a rescue backup and recovery.

But what about the valuable data stored in the SaaS CRM system?

SaaS data needs to be backed up separately from the primary source, by a trusted third party, in order to protect against emerging threats that corrupt, hold ransom, or destroy critical information.

In fact, if you look back over 2017's data breach events, there are several examples to point to involving data protected by cloud providers. For example, the Republican National Committee leak exposed voter data for nearly 200 million United States citizens. That data was housed on the Amazon Web Services (AWS) cloud provider. That breach wasn't even AWS's fault.

This is why the organizations need to "re-think" backup and up-level to a more comprehensive data protection theme.

Consider your entire data footprint

Achieving an overall data protection plan means considering the overall data footprint where the data resides, regardless of physical location. This means thinking beyond on-premises backup systems. SaaS data is often overlooked, perhaps on the belief that the data is already protected—but it really isn't. SaaS vendors strive for reliability, but they are also susceptible to software defects, infrastructure failures, and human error.

As a start, replace "backup" with "data protection" in your IT lexicon. By doing this, you will recognize the need for a more thoughtful and comprehensive plan to protect data. This means:

- A security review of data stored in the cloud
- A review of contingency plans for outages
- Enforcing policies for compliance and data access
- Reviewing SLAs from SaaS/cloud vendors

The bottom line is this: regardless of where your data resides, you must apply all of the same data access and security controls you'd enforce if that data were in your own on-premises infrastructure. A good plan is to evaluate security and data protection technologies that span both on-premises and cloud data to provide a central platform to manage all your organizational data. Taking a unified approach will combine key capabilities and functionality that are essential for effective data protection.

Companies will continue to move more data to the cloud for the benefits to performance, reliability, and elasticity. If you are smart, you'll evaluate your overall data footprint and transform your mentality and approach from traditional back-office IT to a streamlined and easily managed data protection technology stack that covers both cloud and on-premises data.

Protecting data in a hybrid cloud environment

In an era when "data is the new oil," protecting your business's data is a critical element of your storage strategy. Here's how you can keep your customers' information—and your own business—safe and sound.

BY PAUL TIEN | The past few months have been incredibly instructive on the critical importance of keeping one's data safe, be it customer data or your own intellectual property. Data protection itself covers a broad span:

- Physical data protection
- Protection from device failure
- Protection from data loss and breach

Not only is data security important to the success and reputation of your company, but it can also be IT that goes under the bus when a security event occurs. This means that your career is literally on the line. As a result, your storage architecture had better be up to the task of maintaining the integrity of your data store.

Hybrid-cloud architectures provide one of the most secure means of protecting stored data

The good news is that hybrid-cloud storage architecture is one of the best potential solutions for small- and medium-sized enterprises (SMEs) to leverage when security is of paramount importance. It delivers a secure, end-to-end architecture that provides the flexibility of the cloud with the performance of an on-premises solution, while still encrypting data flows from one site to the other.

You might well ask the question: Why can't a data center be made as secure and fault-tolerant as the cloud? The answer is: Clearly it can. However, this is very costly, and while it's affordable for very large enterprises, this option is out of the price range and scope for SMEs. With their scale, cloud providers can afford highly qualified specialists in redundant facility design, network security, and network operations, and they can develop optimized products and processes. Public cloud data centers typically have at minimum SOC-2, ISO 27001, and PCI-DSS compliance and extend to federal compliance standards.

Public cloud providers are starting to apply big data and AI techniques to monitoring their cloud operations looking for leakages and misconfiguration. Only the largest organization can afford or acquire this expertise in-house. Public cloud providers rely on their brand to protect their business and invest accordingly, while many CIOs and IT managers will only be too aware that IT is still often considered a cost center. Hybrid-cloud storage enables SMEs to garner the benefits of cloud scale and efficiency, including the soft benefits of expertise and operational excellence.

With their scale, cloud providers can afford highly qualified specialists in redun–dant facility design, network security, and network operations, and they can develop optimized products and processes.

Physical data protection

Cloud protection starts with physical security protecting against theft, loss, accidents, power failures, and natural disasters. Cloud data centers are physically secure, often in remote areas, with multiply-redundant, backed-up power supplies, and redundant telecom connections. They offer secure building physical security with controlled access, and their size and the nature of storage management makes it near-impossible to identify the physical location or device storing any one organization's data. By comparison, many enterprises at best tend to have a single data center, and SMEs might have only an in-building server room or data closet. Very small companies may just have a NAS sitting unprotected on site.

To protect against physical data loss, it is essential to have a physically separate offsite backup copy. Unsurprisingly, simple data backup to cloud is the oldest application and, until the advent of big data with cloud, one of the largest consumers of cloud storage.

For physical separation, cloud storage is divided into redundancy or availability zones. Users can select from multiple zones within one data center (locally redundant) or data can be duplicated across different data centers in different locations in a region (zone redundant) or in different regions (geo-redundancy). Unlike traditional storage tiering or offsite backup, cloud-based storage is distributed across redundancy zones and handled by the cloud storage system software transparently to users.

Protection from device failure

The next stage is protection from data loss stemming from device failure. No matter the storage medium, there is always the risk of device failure. With HDD it's inevitable, and Flash devices used in SSD will wear out. RAID technology was developed to protect against drive failure, although with very large drives, RAID is increasingly less effective. For traditional storage, best practice in the industry is to follow a 3-2-1 backup strategy—back up to a second device and then back up to offsite. This quickly becomes expensive in both hardware and IT time spent on maintenance—time that could be spent on strategic business initiatives.

A variant of data loss is inadvertent or malicious deletion of data. Over time users, and even IT managers, utilizing file hosting and collaborative solutions such as Dropbox and Office 365, have become so accustomed to cloud reliability that they assume files are always available. However, if a file is deleted it is only available for recovery for a short time. A 2015 study by EMC found the top causes of data loss were accidental deletion (41%), migration errors (31%), and accidental overwrites (26%). To protect against this, several new products that provide cloud backup are becoming available, especially for Office 365.

Data can also be lost via corruption by viruses or ransomware. Ransomware is the most prevalent incident of malware today, per Verizon's 2018 study of business risks. The WannaCry attack is one recent example; and the city of Atlanta, Georgia, is still reeling from a major ransomware attack that crippled the city's applications, from payroll to public transportation.

Using a hybrid-cloud architecture locates the authoritative data storage in the cloud and gains all the benefits of cloud storage while still presenting a traditional on-premises filer interface—with the added advantage that the filer is now no longer a critical, high-maintenance component. Because the filer is just a cache of the cloud data, if it is replaced it will simply replenish with most active files, once accessed.

Data in cloud storage is spread across multiple drives, and data on the drives is managed throughout their lifecycle by the cloud provider to prevent data loss and make failed drive replacement transparent to the user. As noted above, data can also be saved in geo-redundant locations for maximum protection.

For additional protection, the cloud object store can be configured with versioning and made immutable—meaning data can only be written, not erased, although in practice time limits can be set for when erasure is enabled. This ensures that any saved version of the file is always available for recovery.

Disaster recovery/file level recovery

With legacy NAS devices based on hard drives, we know that these drives will inevitably fail, and it's only a matter of time before data must be recovered. As one of the most basic protection mechanisms available, disaster recovery is a storage function that everybody recognizes as an important baseline to have implemented. However, many businesses today are leveraging two different storage backup and disaster recovery (DR) strategies. They have one system for use as primary storage and another separate version for backup and recovery.

Leveraging the hybrid-cloud model streamlines this process significantly, as SMEs use the same cloud storage service for both primary storage and backup/DR. The hybrid-cloud storage architecture consolidates files into a single store. This is especially beneficial for organizations with multiple sites, because it avoids multiple copies being stored on separate file servers for access with the attendant replication costs, active-version headaches, and overhead. With the scalability and falling cost of cloud storage, combined with full namespace visibility and cached cloud filers, it makes sense to just keep every file available in the cloud at all times.

Hybrid-cloud storage services support file-level restore combined with versioning that lets users find prior versions of their files, which means you can restore/backup individual files without having to deal with the whole data store. And all of these have a high-performance connection as part of the on-premise acceleration.

Protection from data loss and breach

The third part of data protection is protection from data breaches incurred through human behavior. Many data breaches and even ransomware incidents start with phishing attacks through social engineering. Another problem, especially with file hosting solutions, is shadow IT, where employees upload restricted data to an unauthorized personal cloud file hosting application such as Google Drive, OneDrive, or Dropbox.

Many of these do not deliver encrypted end-to-end traffic, although this might be expected from more consumer-oriented services. The bigger issue is that all of these services readily facilitate file sharing—but now IT has no knowledge of what files have been shared and with whom. This can easily violate industry compliance measures like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation).

Data breaches remain a significant IT problem, mostly as a result of human error. Although the best prevention centers around training, systems, and process, an ongoing challenge is simply being aware that a breach has occurred. By avoiding shadow IT, investing in audit tools, using identity management tools like Azure AD combined with device management, and encrypting files at rest and in-transit, breaches can be better avoided and identified when they do occur.

With the scalability and falling cost of cloud storage, combined with full namespace visibility and cached cloud filers, it makes sense to just keep every file available in the cloud at all times.

Until recently there was no requirement to report breaches, and they typically only became publicly known when they hit the news. The GDPR changed that and made breach reporting mandatory. The GDPR (which came into effect May 25, 2018) punishes breaches with severe penalties, both monetary and otherwise. It applies not only to organizations located within the EU but also to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. All companies processing and holding the personal data of data subjects residing in the European Union are subject to the GDPR, regardless of their location.

Although most major cloud vendors fully intend to be GDPR-compliant, it's incumbent upon you and your IT organization to ensure that your on-premises and global file system together make for a compliant storage architecture.

Adopting a hybrid-cloud architecture with secure on-premises filers for access and encryption at rest and in transit, utilizing identity and device management and audit capabilities, preventing shadow IT, and limiting how files can be shared and by whom will minimize breaches. In the unfortunate event of a breach, accurate log files, immutable data, and versioning will speed forensics and recovery.

Maintaining security on an ongoing basis—audits/reviews

Of course, once you finally secure your hybrid-cloud storage architecture, there is no guarantee that it will stay that way! Constant vigilance is always warranted, as well as regularly checking on your platform to ensure it's still where it needs to be. As a result, you should perform regular cloud-compliance audits. These audits can span your cloud storage provider (or providers) and your own on-premise architecture piece as well.

In many ways, securing your business's data has become the most critical role for your IT group. As this dynamic market creates even more sophisticated attacks and glaring vulnerabilities, it will be IT's responsibility to stay ahead of the game. A hybrid-cloud storage architecture should smooth that pathway.

Skimping on business data protection could be a costly mistake

A look at the importance of rapid data recoverability and high availability to mitigate the potentially negative business impact of taking shortcuts and relying on cloud partners too much.

BY RICK BRADDY | Data is essential to the smooth operation of any organization. Whether it's data on your products, customers, or competition, you need it to do business. Your software and systems are dependent on the data that's fed into them.

Big data may be gathered by IoT sensors in vehicles and buildings, in smartphones, and from countless other data points to inform big decisions. But at a granular level you also need small pieces of data to function. Without credentials you can't gain access to the big data, contact suppliers, or even tweak the air conditioning system.

Our dependence on data is profound. You might say it's your business DNA, because it's crucial for survival and growth.

Of course, none of this is apparent until something goes wrong. It's when you lose access to data that you realize just how much you need it and how easy it is to take automated access for granted.

The cost of data loss

The potential cost of a data breach is enormous. The global average is $3.6 million, or $141 per data record, according to the IBM-sponsored 2017 Cost of Data Breach Study from the Ponemon Institute. Those figures were calculated before the General Data Protection Regulation (GDPR) came into effect—with non-compliance potentially leading to fines of up to 20 million euros ($23.3 million) or 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

When data is stolen or lost, companies often struggle to get back on track. Downtime is disastrous for any business—it can't take orders, customers are up in arms, and nothing can be shipped. Not only is there the cost of any punitive fines for regulatory breaches to consider, but also the data itself still has to be recovered and the threat that led to the incident must be mitigated. Only then can the hard work of repairing damaged reputations begin.

Consider that 56 data records are lost or stolen every second, according to the Breach Level Index, and you have some idea of the scale of the problem.

Concealed in the cloud

There are lots of sound business reasons to embrace the cloud. It offers rapid scalability and flexibility, enabling organizations to

If you are keen to leverage the potential of the cloud, it's crucial that you're aware of the potential pitfalls of cloud data management.

focus on what truly differentiates them in the marketplace, but the rush to migrate has led to some dangerous shortcuts.

Shadow IT—things that go beyond the watchful eye or direct control of IT departments—represents a serious security risk. We're talking about more than 50 percent of IT spending for many large enterprises, according to the Everest Group.

If you are keen to leverage the potential of the cloud, it's crucial that you're aware of the potential pitfalls of cloud data management. Take the time to plan your migration properly, assess what data is critical for your operations, and take steps to protect it and make it highly available and rapidly recoverable.

Understand that you can't rely solely on cloud vendors to safeguard your data and application availability.

The race to recover

The per day, hour, or even minute cost of downtime varies from company to company, but what we can say with confidence is that every organization that suffers an incident wants to get back up and running as fast as it possibly can. If there are no storage snapshots to clone and quickly bring back online or a recent backup that can be swiftly accessed, then there's a very real risk that you're going to lose valuable data permanently.

Even if you have an older backup and decide to recover that, you may find that configurations are out of date, passwords no longer work because they've been changed, and business records and accounts are gone. Think about how you would deal with an incident like that if the data proved irrecoverable. The cloud vendor may be to blame, but your management team, your customers, and the regulatory bodies will still hold you accountable.

The faster you can recover, the better the chances are your business will survive, but the truth is that major data breaches are often bad enough to take down entire companies.

Weighing it up

Organizations often skimp on backups and redundancy to save money, but that's a false economy based on short-sighted thinking. It's not possible to build impenetrable defenses, and even if it was, it would be prohibitively expensive. But let's say your cybersecurity is that strong. It's still possible for an employee to accidentally delete something of vital business importance. It's possible for hardware underpinning cloud systems to fail.

The chances are high that your business will suffer from data loss or theft at some point. When Bitdefender surveyed 250 IT decision makers, 34 percent of them reported breaches within the last 12 months and 74 percent of them couldn't identify the cause of the breach. Accept that you can't fully prevent data breaches from happening and plan accordingly.

If a few thousand dollars seems too expensive right now, try to calculate the potential cost of an irrecoverable loss of business-critical data or of many days of extended downtime. We pay insurance premiums because the cost of an incident can be catastrophically high. The same logic applies to data protection and high availability in the cloud. Properly insulated, high-availability, regular backups and replication, and the right data protection mechanisms baked in from the start, can be the difference between recovering from a malware infection, ransomware attack, or unexpected cloud service failure—and not recovering at all.

Cloud backup is not the same as standard data center backup

You must implement some sort of cloud-based system recovery, with varying costs and risks.

BY DAVID LINTHICUM | Backup is just good policy. You need the ability to back up data and applications someplace, so they can be restored somehow, to keep the business running in case of some natural or manmade disaster that takes the primary business-critical systems down.

We have whole industries that provide backup sites and backup technology. They can be passive, meaning that you can restore the site in a short period of time and get back to operations. Or they can be active (which costs more), meaning it can instantly take over for the disabled systems with current data and code releases—in some cases, without the users even knowing.

In the cloud, disaster recovery involves a new set of choices that don't look much like the ones you have for on-premises systems. The approach that you take should represent the value that the applications and data sets have for the business. I suggest that you look at the practicality of it all, and also make sure that you're not spending more than the disaster recovery configuration is worth.

Option 1: Region-to-region disaster recovery

You can set up two or more regions in the same public cloud provider to provide recovery—so if the Virginia region is taken out, for instance, there are other regions in the country that take over.

You can pay to have exact copies of the data and apps replicated to the backup region, so they can seamlessly take over (that's active recovery). Or you can use more cost-effective approaches, such as scheduled backup to passive mass storage, to stand up the other region quickly (that's passive recovery).

Option 2: Cloud-to-cloud disaster recovery

The most common questions that I get are: What if the entire public cloud provider is wiped out? In a long-term outage, how can we protect ourselves?

Using one public cloud to provide backup to another public cloud would let you, for example, use Amazon Web Services to back up Azure, go the other way around, or do some other pairing.

While this seems like the ultimate in disaster recovery—and in hedging bets—doing multicloud just to support disaster recovery means keeping around two different skill sets, having two different platform configurations, and other costs and risks.

Ongoing cloud-to-cloud system replication (aka intercloud replication) increases the chance that things will go wrong. That's not what you want when trying to replicate the primary and backup platforms. While it's not impossible, intercloud replication is five times more difficult than intracloud replication within the same provider. That's why intercloud support is almost nonexistent, outside a few clever consultants.

In the cloud, disaster recovery involves a new set of choices that don't look much like the ones you have for on-premises systems. The approach that you take should represent the value that the applications and data sets have for the business.

7 common cloud data management pitfalls to avoid

What to watch out for as you migrate data to the cloud.

BY RICK BRADDY | There are many compelling reasons to migrate applications and workloads to the cloud, from scalability to easy maintenance, but moving data is never without risk. When IT systems or applications go down, it can prove incredibly costly for businesses. A single hour of downtime costs over $100,000, according to 98% of organizations surveyed by ITIC.

Mistakes are easy to make in the rush to compete. There's a lot that can go wrong, particularly if you don't plan properly.

"Through 2022, at least 95% of cloud security failures will be the customer's fault," says Jay Heiser, research vice president at Gartner.

If you want to avoid being in that group, then you need to know about the pitfalls to avoid. To that end, here are seven traps that companies often fall into.

#1 No data-protection strategy

It's vital that your company data is safe at rest or in transit: you need to be certain that it's recoverable if disaster strikes. Consider the threat of corruption, ransomware, accidental deletion, and unrecoverable failures in cloud infrastructure. If the worst happens, and you expect more than an apology or a refund, then a coherent, durable data protection strategy is essential. Put it to the test to make sure it works.

#2 No data-security strategy

It's common practice for the data in a data center to be comingled and co-located on shared devices with countless unknown entities. Cloud vendors may promise that your data is kept separately, but regulatory concerns demand that you make sure. Think about access control, because basic cloud file services often fail to provide the same user authentication or granular control as traditional IT systems. The Ponemon Institute puts the average global cost of a data breach at $3.6 million. You need a multi-layered data security and access control strategy to block unauthorized access and ensure your data is safely and securely stored in encrypted form, wherever it may be.

#3 No rapid data-recovery strategy

With storage snapshots and previous versions managed by dedicated NAS appliances, rapid recovery from data corrup-

You need a multi–layered data security and access control strategy to block unauthorized access and ensure your data is safely and securely stored in encrypted form, wherever it may be.

tion, deletion, or other potentially catastrophic events was possible. But few cloud-native storage systems provide snapshotting or offer easy rollback to previous versions, and that leaves you reliant on current backups. You need flexible, instant storage snapshots that provide rapid recovery and rollback capabilities for business-critical data and applications.

#4 No data-performance strategy

A shared, multi-tenant infrastructure can lead to unpredictable performance, and many cloud storage services lack the facility to tune performance parameters. Too many simultaneous requests, network overloads, or equipment failures can lead to latency issues and sluggish performance. Look for a layer of performance control for your data that enables all your applications and users to get the level of responsiveness that's expected. You should also ensure that it can readily adapt as demand and budgets grow over time.

#5 No data-availability strategy

Hardware fails, people commit errors, and outages are an unfortunate fact of life. It's best to plan for the worst. Create replicas of your most important data and establish a means to quickly switch over whenever sporadic failure comes calling. Look for a cloud or storage vendor willing to provide an SLA guarantee for your business. Wherever necessary, create a failsafe option with a secondary storage controller to ensure your applications do not experience any outage.

#6 No multi-cloud interoperability strategy

As many as 90% of organizations will adopt a hybrid infrastructure by 2020, according to Gartner analysts. There are plenty of positive driving forces as companies look to optimize efficiency and control costs, but you must properly assess your options and the impact on your business. Consider the ease with which you can switch vendors in the future and any code that may have to be rewritten. Vendors want to entangle you with proprietary APIs and services, but you need to keep your data and applications multi-cloud-capable to stay agile and preserve choice.

#7 No disaster recovery strategy

A simple mistake where a developer accidentally pushes a code drop into a public repository and forgets to remove the company's cloud access keys from the code could be enough to compromise your data. Maybe your provider will be hacked and lose your data and backups. It's critically important to keep redundant, offsite copies of everything required to fully restart your IT infrastructure in the event of a disaster or full-on hacker attack break-in.

The temptation to cut corners and keep costs down with data management is understandable, but it's short term thinking that could end up costing you a great deal more in the long run. Take the time to craft the right strategy, and you can drastically reduce the risk.

What is disaster recovery? How to ensure business continuity

Organizations prepare for everything from natural disasters to cyber-attacks with disaster recovery plans that detail a process to resume mission-critical functions quickly and without major losses in revenues or business operations.

BY KEITH SHAW | Disasters come in all shapes and sizes. It's not just catastrophic events such as hurricanes, earthquakes, and tornadoes, but also incidents such as cyber-attacks, equipment failures, and even terrorism that can be classified as disasters.

Companies and organizations prepare by creating disaster recovery plans that detail actions to take and processes to follow to resume mission-critical functions quickly and without major losses in revenues or business.

What is disaster recovery?

In the IT space, disaster recovery focuses on the IT systems that help support critical business functions. The term "business continuity" is often associated with disaster recovery, but the two terms aren't completely interchangeable. Disaster recovery is a part of business continuity, which focuses on keeping all aspects of a business running despite the disaster. Because IT systems these days are so critical to the success of the business, disaster recovery is a main pillar in the business continuity process.

The cost of disasters

Economic and operational losses can overwhelm unprepared businesses. One hour of downtime can cost small companies as much as $8,000, midsize companies up to $74,000, and large enterprises up to $700,000, according to a 2015 report from the IT Disaster Recovery Preparedness (DRP) Council.

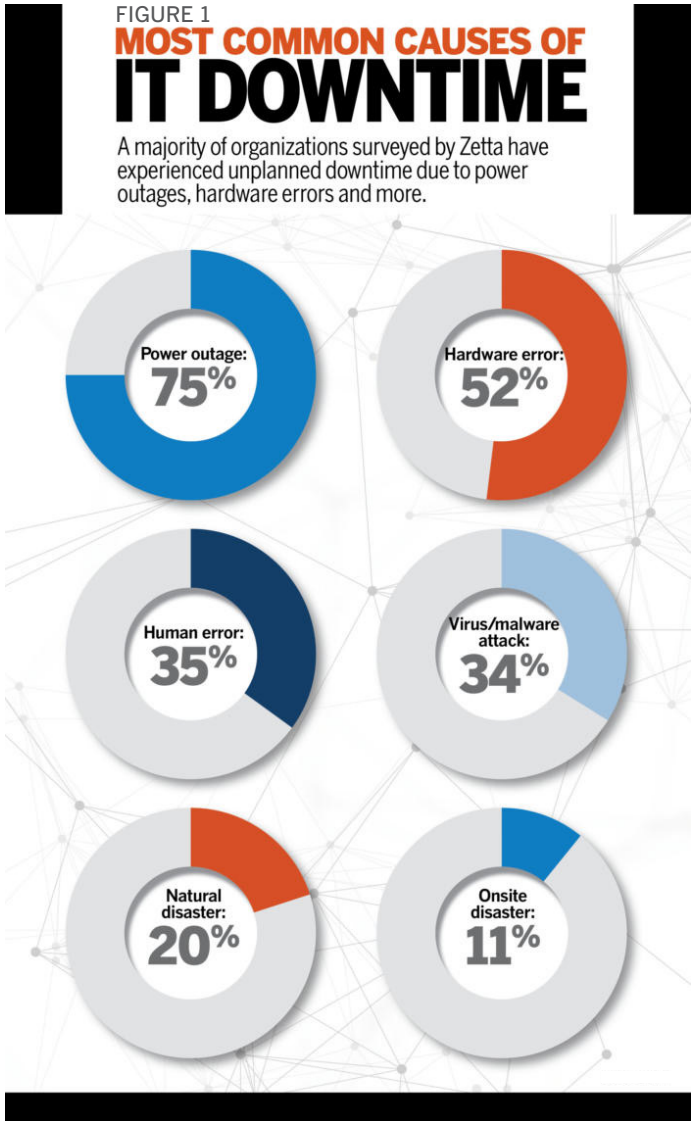
Another survey from disaster recovery service provider Zetta showed that more than half of companies surveyed (54%) had experienced a downtime event that lasted more than eight hours over the past five years. Two-thirds of those surveyed said their businesses would lose more than $20,000 for every day of downtime.

Risk assessments identify vulnerabilities

Even if your company already has a disaster recovery plan of some sort, it may be time for an update. If your company doesn't

Disaster recovery is a part of business continuity, which focuses on keeping all aspects of a business running despite the disaster.

FIGURE 1



SOURCE: ZETTA

have one, and if you've been handed the task of coming up with one, don't jump in feet first without doing risk assessment. Identify vulnerabilities to your IT infrastructure and where things could go wrong. A prerequisite is knowing what your IT infrastructure looks like.

Knowing where things could go wrong doesn't mean that you start creating worst-case-scenario plans. In a recent blog post in the *Disaster Recovery Journal*, authors Tom Roepke and Steven Goldman suggest that naming the worst-case scenario in business continuity planning can be dangerous because it draws attention away from other significant threats:

"The natural tendency is to try to name or define what the worst-case scenario is. This becomes a fatal flaw because it shapes the entire planning effort thereafter, even if it is at a subconscious level. So when we insert a named scenario—pandemic, earthquake, cyber-attack, etc.—we automatically start thinking and planning in terms of response/recovery for that specifically and subconsciously defined incident. When this occurs we not only tend toward a tunneled view in our planning efforts, but we are also in danger of increasing our risk and exposure. This is because there will be a hyper-focus on only one or two specific areas in what we think is the worst-case scenario, and not the actual event."

The key, Roepke and Goldman suggest, is to focus on "managing the crisis, restoring business-critical functions, and recovering, all while communicating with your stakeholders."

What is a disaster recovery plan?

Type "disaster recovery plan template" into Google and dozens, if not hundreds, of templates will appear. Use those to get started and modify towards your business or organization.

The plan itself should include the following:

- Statement, overview, and main goals
- Contact information for key personnel and disaster recovery team members
- Description of emergency response actions immediately following a disaster
- Diagram of the entire IT network and the recovery site. Don't forget to include directions on how to reach the recovery site for personnel who need to get there.
- Identifying the most critical IT assets and determining the maximum outage time. Get to know the terms Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO indicates the maximum "age" of files that an organization must recover from backup storage for normal operations to resume after a disaster. If you choose an RPO of five hours, then the system must back up at least every five hours. The RTO is the maximum amount of time, following a disaster, for the business to recover its files from backup storage and resume normal operations. If your RTO is three hours, it can't be down longer.
- List of software, license keys, and systems that will be used in the recovery effort
- Technical documentation from vendors on recovery technology system software
- Summary of insurance coverage
- Proposals for dealing with financial and legal issues, as well as media outreach

Building a disaster recovery team

The plan should be coordinated by IT team members responsible for critical IT infrastructure within the company. Others who need to be made aware of the plan include the CEO or a delegated senior manager, directors, department leaders, and human resources and public relations officials.

Outside the company, vendors associated with disaster recovery efforts (software and data backup, for example) and their contact information should be known. Facility owners, property managers, law enforcement contacts, and emergency responders should also be known and listed within the plan (and updated frequently as names or phone numbers change).

Once the plan is written and approved by management, test the plan and update if necessary. Be sure to schedule the next review period and/or audit of the disaster recovery functions. Update, update, update as events transpire (large or small). Don't just put the plan in a desk drawer and hope that a disaster doesn't occur.

A disaster has happened—now what?

If a disaster has occurred, it's time to start your incident response. Make sure that the incident response team (if it's different from the disaster recovery planning team) has a copy of the disaster recovery plan.

Incident response involves assessing the situation (knowing what hardware, software, or systems were affected by the disaster), recovery of the systems, and follow-up (what worked, what didn't work, what can be improved).

What's next? Cloud or recovery-as-a-service

Like many other enterprise IT systems that have moved to the cloud, so has disaster recovery. Benefits of the cloud include lower cost, easier deployment, and the ability to test plans regularly. However, this could come with increased bandwidth needs or degrade a company's network performance with more complex systems.