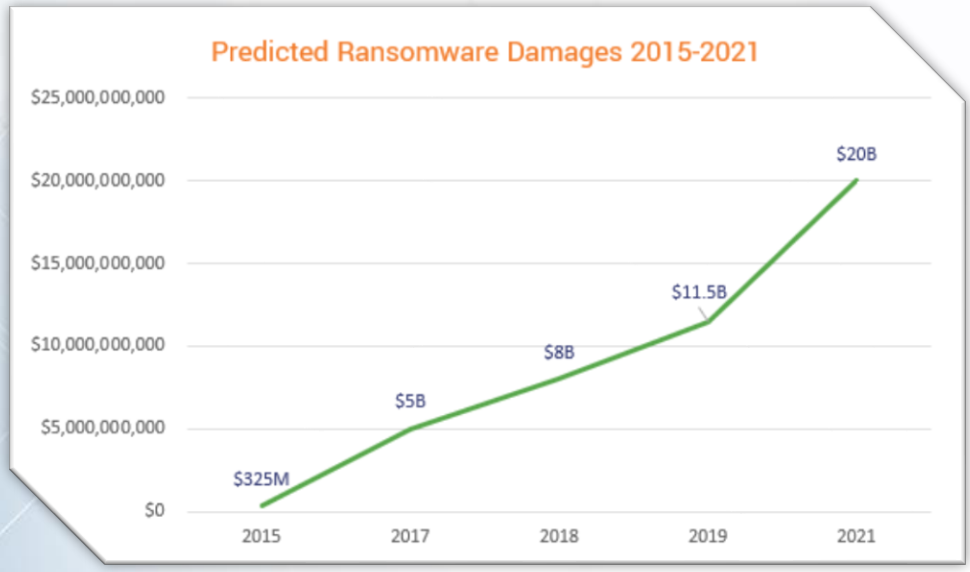
HOW DISASTER RECOVERY IS THE ANSWER TO RANSOMWARE

How Disaster Recovery is the Answer to Ransomware

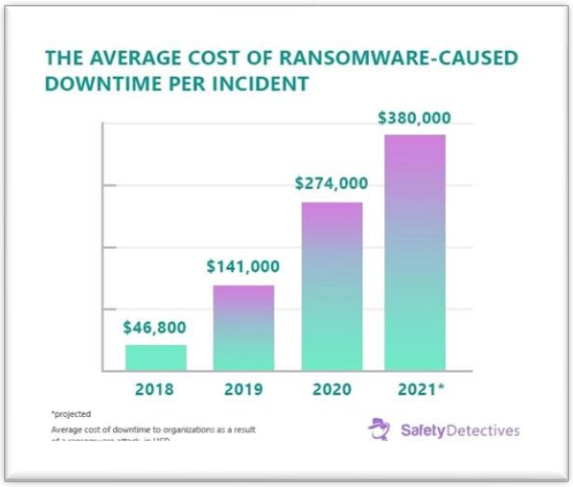
Ransomware attacks are increasing at a startling rate. Ransomware is a type of malware that prevents users from accessing their systems or personal files, and demands a ransom payment to regain access to their files or system. Ransomware is a nightmare for unprepared IT administrators. No industry or organization is safe from ransomware attacks: healthcare, sports, manufacturing, banks, and government institutions all have been the victims of such vicious attacks.

Ransomware is a multibillion-dollar operation and all the IT security vendors are fighting the perpetrators of ransomware attacks. Nevertheless, no IT system is safe from such a threat. Ransomware attacks are going to steal roughly $20 billion off global organizations in 2021, according to Cybersecurity Ventures. This is an increase from their earlier estimated damage of $11.5 billion for 2019 and $8 billion for 2018.



Most of the companies across the globe are going through data loss and major downtime due to ransomware attacks. These outcomes prove to be very costly, especially for bigger organizations with hundreds of employees. The average cost of ransomware-caused downtime is doubling right now.

Disaster Recovery is the last line of defense in this regard. Disaster Recovery refers to the procedures, policies and processes that prepare the IT infrastructure of an organization to recover from natural or human-induced (malware) disasters and ensure business continuity. A disaster recovery plan (DRP) represents how an organization will respond to any potential disaster situation, to support time-sensitive business processes and maintain full business continuity.



The disaster recovery plans encompass both responsive and preventive fronts. The responsive front represents different disaster situations and explains the detailed responses to each, to reduce the negative impact. The preventive front represents the main objective of reducing the negative impact of any disaster situation by explaining what the organization has to do to avoid such disasters.

Disaster recovery relies on the replication of data and computer processing in an off-premises place, which is not affected by the disaster. As the servers go down in a disaster situation such as an equipment failure or a cyber-attack, a business organization is required to recover the data from a second location where the data is backed up. An organization can transfer its computer processing to that second location so that its operations continue to function. There are five main elements of a disaster recovery plan.

01

Disaster recovery team

It includes a group of specialists responsible for creating, implementing and managing the disaster recovery plan.

02

Risk evaluation

It refers to the assessment of potential risks to the organization. It also strategizes the type of measures that are required to resume business.

03 **Business-critical asset identification**

It refers to the documentation of all the critical and sensitive data, files, systems and applications.

04 **Backups**

It evaluates what is required to backup, who should perform the backup and how to implement backup.

05 **Testing and optimization**

The recovery team is required to upgrade its strategies to control ever-increasing threats to the organization's data security.

There are different methods of disaster recovery being employed by businesses and organizations such as backup management, cold sites, hot sites, backup as a service, virtualization, data center disaster recovery, and disaster recovery as a service (DRaaS). Disaster recovery as a service is being employed in major organizations against malware attacks. It is effectively resolving the situations created after malware attacks.

Disaster recovery as a service (DRaaS) refers to a cloud computing service model that helps an organization to back up its data and IT infrastructure in a third-party cloud computing environment, offering the whole disaster recovery through a SaaS solution, thus regaining access and functionality to its IT infrastructure after a disaster. It involves third-party hosting and replication that offers full recovery with SLAs defining the DRaaS provider's role and recovery timings. This is a perfect model for the organizations lacking resources to provision, configure and test their DR plans in-house and maintain their own off-site DR environments. DRaaS is also particularly effective for organizations with minimal tolerance for downtime.

The striking feature of DRaaS is its short recovery point objective. It means that in case of a disaster such as a malware attack, the data restored through DRaaS will be as close to its current 'now' state as possible. The typical time recovery objectives of DRaaS is 4 hours. It brings up machines geographically located in different locations. For example, if a hurricane affects an organization's data center in Hawaii, DRaaS ensures that the data will not be lost by switching to live mirrored servers in Georgia, which were not harmed by the hurricane.

There are three major models of DRaaS.

01

Managed DRaaS

In this model, the third party takes full responsibility for disaster recovery. The organization choosing this model needs to be in close contact with the DRaaS provider to ensure that it stays up to date on the infrastructures, applications, and service changes. It is best for organizations lacking the time and expertise required for disaster recovery.

02

Assisted DRaaS

Assisted DRaaS is a good option for organizations that want to give partial responsibility for disaster recovery to the DRaaS provider and keep partial responsibility to them. In this model, the service provider provides the expertise for disaster recovery and the responsibility of implementing some or full recovery plan.

03

Self-Service DRaaS

It is the least expensive model of DRaaS. The customers are responsible for planning, testing, and management of disaster recovery. The customers are required to host their infrastructure backup on virtual machines in a remote location. Organizations with experienced disaster recovery staff can easily hire such a model.

Disaster recovery plans are changing the fates of businesses and organizations in case of cyberattacks such as ransomware attacks. According to a study, 96% of businesses with disaster recovery plans recover their operation completely, in case of any nature of man-induced attacks (disasters).

Statistics by *FEMA* show that 40-60% of small businesses who lose access to operational systems and data without a DR plan have to close their businesses. Recovery of data after an attack or disaster should be fast, or it will have a dire effect on the organization. DRaaS provides such a service and ensures the availability of all the lost data due to a disaster. However, 9 out of 10 small organizations who suffer from a disaster fail within the following year, as they do

not have any recovery plans in place. According to Datto, a small company suffers a loss of around $8,500, a medium company of $78,000, and a large enterprise suffers a loss of $740,000 for the downtime of one hour.

Therefore, disaster recovery plans and services are essential for businesses and organizations. They offer the infrastructure and expertise required to get out of a disaster situation and recover valuable data.

The global Disaster Recovery as a Service market is estimated to grow from $5.1 billion in 2020 to $14.6 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 23.3% during the forecasted period.

DRaaS ensures the recovery of company information after natural disasters, cyber or physical attacks, user errors, hardware failures, or any other event that results in data loss.

"I was tasked with finding an impenetrable managed IT service, and I did my homework and made a lot of phone calls and did a lot of intros, and I circled back around to my partnership with EstesGroup and realized that they had exactly what I was looking for."

Bryan Provo, President, Alliance Machine Inc