VEEAM | UBX CLOUD

think teal™

A Think Teal Insights Paper

RESILIENCE UNLEASHED

Mastering BCDR Strategies in the Age of Ransomware

Today, most of us are familiarized with the term “Digital Economy”. Businesses in the developing and developed nations use this term to identify the digital transformation initiatives that is propelling their growth across different areas. The growing maturity in technologies like mobility, cloud computing, artificial intelligence and analytics is driving most of the businesses to take up digital transformation initiatives. One of the most important aspect that is pushing digital transformation forward is the “Data”. Businesses today are embracing different technologies in order to use the large volumes of data generated and build meaningful insights out of them which will help them excel in business. Data has become a bedrock on which all the people, process and technology aspects of businesses are becoming reliant.

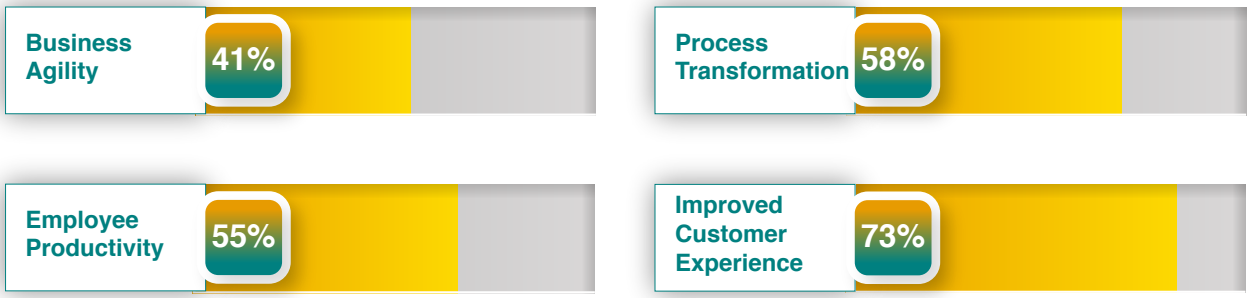
DATA FORMS THE “BEDROCK” ON WHICH EVERY ASPECT OF DIGITAL TRANSFORMATION IS DESIGNED TODAY

In the age of Internet, global businesses are exploring new investment opportunities and are pushing capital into emerging economies and are actively investing in new technologies to have a competitive advantage and to excel in their strategic business objectives. With emergence of new technologies, there is rapid growth happening across all the digital products and services that is being offered by businesses that are being developed using data being collected using different sources. The concept of Internet of Things, social media and Internet connected user devices is giving rise to large volumes of data. This data obtained from various sources are being used by businesses to build business intelligence which is proving critical in the digital transformation journey of organizations. The data generated is also helping companies to bring reform different aspects of business be it the internal factors like employee experience or to enhance external business parameters like customer experience.

Businesses today are dealing with completely new set of challenges than what they were dealing with a decade ago. In this evolving scenario having a data driven agile business helps organizations to be prepared in all the scenarios. To achieve business efficiency and to fulfil business objectives as well as organizational objectives, businesses need to focus on using data efficiently. CIOs and IT decision makers, through digital transformation initiatives want to achieve business agility, enhance employee productivity, implement business process transformation and most importantly, drive greater customer satisfaction. Data today is becoming one of the most important assets for organizations and companies do not want their core business to be impacted in the process of digital transformation. IT leaders and companies are well aware that while having a digital transformation roadmap is the need of the hour, they also do not want to leave their organization's data exposed to any unwanted vulnerabilities.

When we asked our CIO community as to why they want to pursue their digital transformation efforts, most businesses said they wanted to enhance their customer engagement efforts. While they pointed to different business as well as operational objectives they want to achieve, they at the same time highlighted what are their expectations with respect to the security posture is in their digital transformation journey.

BUSINESS & OPERATIONAL OBJECTIVES
CIOS WANT TO ACHIEVE



While the IT decision makers see digital transformation as an important business imperative, they do not want their precious data to be exposed to external threats. As businesses continue to digitize their overall business processes, concepts like bring your own device (BYOD), anytime-anywhere work flexibility, access to company's digital information are posing security related challenges that businesses want to avoid.

Companies today want to tread cautiously in their digital transformation journey. Many of the businesses that have initiated digital transformation processes without revisiting their IT security posture have known to be exposed to data security threats. Businesses today are in no position to lose their data to cyber-attacks. Such attacks not only bring financial losses to the company but also dent the reputation of organizations. If the data losses are irrecoverable and if there are sensitive customer information that businesses tend to lose, businesses have the possibility of completely losing its track and end up falling to a level where they can never recover. Hence, companies today are more critical about safeguarding their data and maintain right balance between their digital transformation progress and enhance their security measures to suit modern day business requirements.

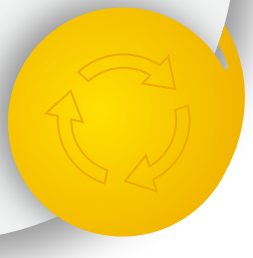
SECURING THE BUSINESS – BECOMES PRIORITY TO ACHIEVE THESE OBJECTIVES

73%

said they want to mitigate cyber attacks that they might encounter during the DT Journey

71%

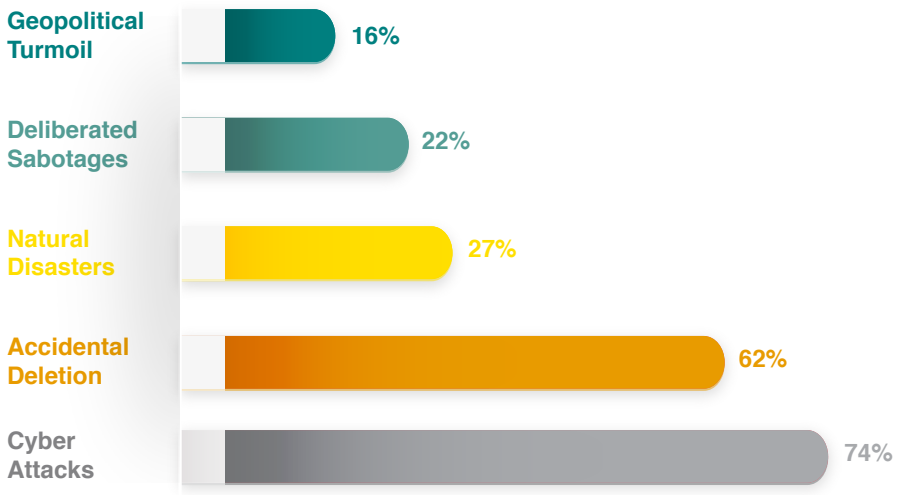
CIOs agree that their business continuity should remain intact in order make digital transformation successful



Digital Transformation Enhances Efficiency – But Brings Greater Security Risks

While there is no second thought about how digital transformation can enhance the overall business processes within an organization, it also brings with it greater security threats as businesses are compelled digitize most of their processes. In their journey of digital transformation, most businesses tend to miss updating their security posture in-line with the digitization efforts that they are carrying out. As a result, the businesses processes get digitally transformed but security aspects remain outdated thereby attracting cyber criminals. When we asked our CIO community as to what was one of those main causes of businesses disruptions in today's digitizing business world, most of the respondents pointed to cyber-attacks. It is interesting to note that a couple of decades ago, when businesses were not so digitally sound, the number of cyber-attacks were limited and business disruptions were mostly due to geo-political unrest or other natural calamities.

SOME OF THE MAJOR CAUSES OF BUSINESS DISRUPTIONS TODAY



In recent years, as businesses are continuing to digitize their business, the cyber criminals are finding innovative ways to breach the security apparatus in place. As businesses are trying to revamp their security infrastructure to match today's business requirements, cyber miscreants are staying one-step ahead and finding innovative methods to access company information. With the recent push for flexible work environment, easy access of company information to employees and greater importance being given to digitization of business processes, it is becoming increasingly simpler for attackers to find loopholes within the business processes and exploit them accordingly.

CYBER CRIMINALS FINDING EASY & UNIQUE WAYS TO DISRUPT BUSINESS

Ransomware – Growing Notorious among all the Attacks

Some of the common methods which attackers are employing to breach security measures of the organization include identity based attacks where miscreants mask their identities and try to steal information. In recent years, Ransomware attacks have become rampant as attackers are finding it to steal data for a ransom and threaten companies with leaking of data on dark web if the ransom hasn't been paid. Ransomware attacks were number one threat in 2022 and 1 out of ever 4 cyber-attacks were ransomware based attacks.

CYBER CRIMINALS ARE USING "THREATS OF DATA LEAK" TO PRESSURIZE COMPANIES TO PAY RANSOM

Nearly **90%** of the companies have reported one or more instances of Ransomware attacks in the past **12 months**

55% of the businesses paid ransom to prevent **revenue losses**

More than **50%** of the IT Professionals have reported **increase in ransomware** attacks compared to previous year

More than **45%** of the businesses **did not have a proper backup plan and suffered data loss** when recovering from a ransomware attack

Ransomware attacks do not just threaten to harm the data integrity of an organization but also negatively impacts the tangible and intangible assets of the organizations. There has been instances where companies have suffered losses to their businesses to a point where they have not been able to recover. Ransomware attacks today are evolving and cyber criminals are using methods that can easily bring business to a standstill.

Organizations globally have been familiar with ransomware attacks for years. In the recent years, the number of companies that were affected with ransomware attacks has reached its peak level. Moreover,

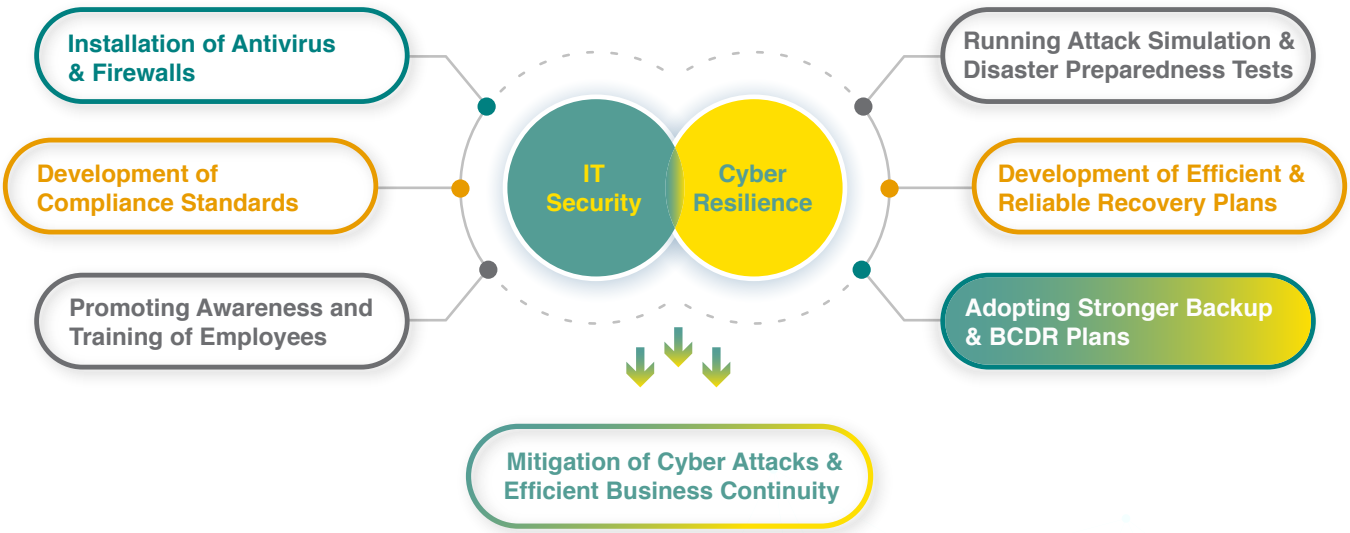
these attacks are increasingly becoming sophisticated. Introduction of new methods of blackmailing organizations for ransom, availability of ransomware related kits and introduction of innovative methods like Ransomware-as-a-service has added to the complications of organizations.

Security leaders in the past have firmly believed that investing in point products for enhancing security posture was an effective way to tackle ransomware attacks. However, as per research and past instances, businesses that relied on these point products were most likely to be affected by ransomware attacks. As attackers continue to employ aggressive strategies, organizations are realizing the need for investing in right technologies, people and processes will be the only way forward to effectively deal with ransomware type of attacks. The frequency of ransomware attacks continue to grow and businesses need to find better synergies between their IT security strategies and their over cyber resilience roadmap. Most businesses do not have their cyber security strategies aligned and in some cases do not have any cyber resilience roadmap as such. This eventually makes fighting ransomware attacks a complex task.

IT Security + Cyber Resilience – Answer to Ransomware Attacks

With growing incidents of ransomware attacks, it is increasingly becoming imperative for organizations to have a aligned IT security and cyber resiliency strategy. Having this alignment helps organizations to build multi-pronged security policy and processes that is critical in fighting cyber-attacks in general.

ENTERPRISES OFTEN TEND TO IGNORE BUILDING CYBER RESILIENCE STRATEGY AND FOCUS ONLY ON HAVING CYBER SECURITY MEASURES IN PLACE



IT security forms an immediate response to any ransomware types of attacks which involves activation of different cyber security measures like antivirus and firewalls and development of a pre-set compliance standards that businesses need to follow to effectively deal with any cyber threats. IT security measures also involve promoting awareness among employees and training them on how to deal with potential threats and unusual activities that they might come across.

Cyber resilience on the other hand is a well thought approach combining several measures, policies and processes that businesses have to develop over a period of time to deal with potential attacks. Cyber resiliency strategy necessarily involves running attack simulation and disaster preparedness tests at regular intervals of time and collecting information on how the measures can be further strengthened to deal with untoward attacks. It also involves development of efficient and reliable recovery plans that will help organizations to stay get back to normalcy in case of any attacks and consequent business disruptions.

Another important aspect of cyber resiliency strategy is adoption of strong backup and BCDR plans. In case of any ransomware attacks, having effective backup plans would mean the copy of the data remain intact and businesses can continue to stay afloat and thereby avert any financial as well as business losses. Having backups that are safely protected and in isolation from the main business processes minimizes impact of ransomware and ensures business continuity no matter what. In recent years, the need for having strong BCDR plans that can effectively deal with ransomware attacks is increasingly becoming critical for businesses.

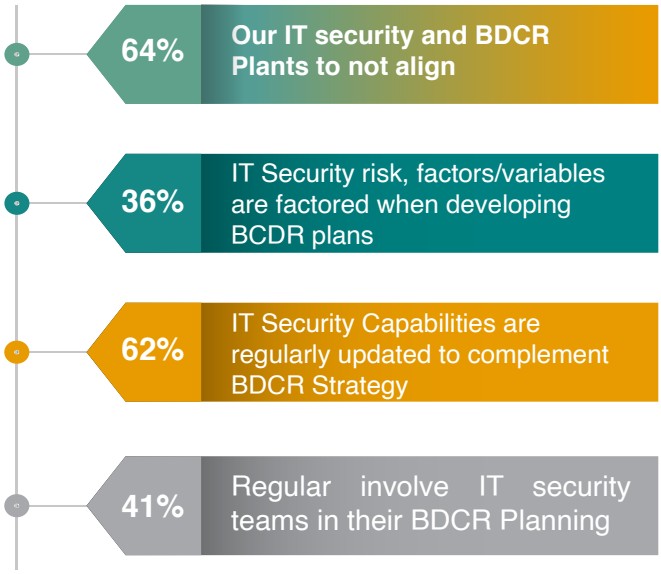
Aligning IT Security and BCDR Strategy – A Challenging Task

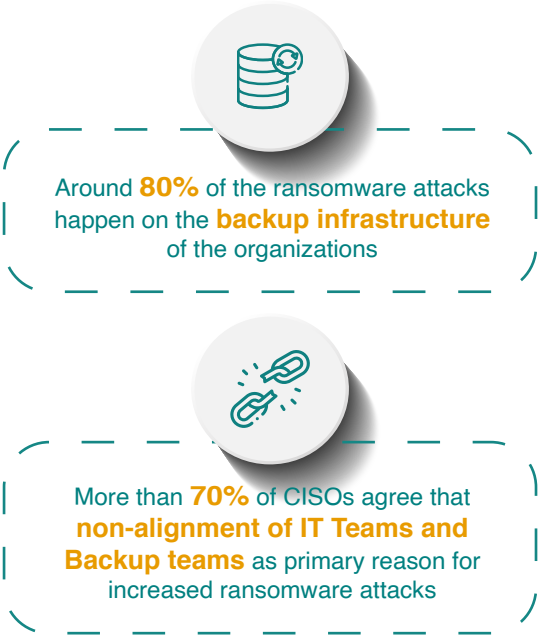
Although it is ideal to have a aligned BCDR and IT strategy in place, most of this alignment are largely limited to papers. Research say that most businesses do not have any alignments of such kind and the IT security teams and BCDR functions work in silos thereby attracting potential threats which otherwise can be avoided. When we asked CIOs how their IT security strategy and BCDR strategy complement each other, most respondents revealed that they do not have any such strategy in place.

With non-alignment of cyber security and BCDR strategies, it becomes easy for cyber criminals to conduct attacks on backup infrastructure. With security of the backup infrastructure compromised, attackers will get easy access to critical backup data which they can block and can ask organizations to pay to release this data. With backup getting compromised, it becomes almost impossible for businesses to ensure business continuity. As a result, the company can witness not just financial losses due to loss of data but also due to business coming to a standstill. Apart from the financial losses businesses can also experience reputational loss which can be damaged to an extent where it becomes irreparable.

IT SECURITY TEAMS AND BCDR FUNCTIONS WITHIN ORGANIZATIONS TEND TO WORK IN SILOS – THIS HELPS CYBER CRIMINALS TO EASILY EXECUTE RANSOMWARE ATTACKS

Current Trends in Organizations with respect to IT Security and BCDR Strategy





How a Ransomware Focused BCDR Plan Helps

Businesses have been familiar with the concept of backups for decades. Most of the businesses today employ different backup solutions in order to replicate their data to safe locations. The need for continuity of business cannot be achieved by having just a backup solution. As businesses continue to expand and as their reputation in the market continues to soar, being available to customers and other stakeholders is increasingly becoming important. BCDR is one such strategy that is helping organizations to stay afloat all the time.

A ransomware focused BCDR plan helps organizations to take a holistic approach towards data protection. BCDR essentially covers strong elements of data protection. Additionally, BCDR also has some of the critical components of cyber security. This makes BCDR a strong strategy that business needs to integrate in their data protection plans in order to fight ransomware attacks. BCDR today is revolutionizing the data protection approach and backup processes of organizations and thereby enabling them to achieve greater resiliency, efficiency and security. Business owners are adopting BCDR plans as they are formulated to make backups more reliable than ever and optimize recovery time when there any business disruptions due to attacks like ransomware.

An important aspect of storage infrastructure today is its security capabilities. Many businesses today do nor regularly update their overall enterprise security posture. As a result, infrastructural assets like storage

are mostly the ones that get impacted. With growing data and weaker security capabilities, storage infrastructure become highly vulnerable. To address this issue, modern storage solution providers are introducing several new security capabilities that can help organizations to keep their storage infrastructure free from any cyber-attacks.

HAVING BCDR SOLUTION DURING RANSOMWARE MEANS AN ADDITIONAL PLAN TO KEEP ORGANIZATIONS RUNNING – NO MATTER WHAT

Having no backup and BCDR plan in place can make business vulnerable. Many companies, even today, do not have an answer to what would be their strategy if there is a cyber-attack and the attack breaches the cyber security measures that is in place. In most of the cases, businesses do not foresee the risks associated with not having a well thought BCDR plan. IT security strategies of some companies do not upgrade as they evolve. As a result, businesses are not aware of the security risks they are being exposed to. And when the disaster strikes, they will be taken aback and would realize the damages they have gone through.

On the other hand, having a strong BCDR plan would act like a second line of defence where after an attack, as a part of the IT Security measures in place, the firewalls, intrusion detection and prevention systems get activated and if the nature of attacks are severe and standard cyber security measures are not able to handle these attacks, the existence of a proper BCDR solution enables organizations to have second line of defence and protect data assets of organizations from further damage. While the security solutions in place enables organization to contain the spread of attack, backup and recovery solution will help organization to re-cover data that has been held ransom through a BCDR solution and this in turn helps businesses to stay up and running even when there is any disruption. BCDR solutions that are clearly aligned with the IT cyber security of organization helps businesses to minimize the impact of attacks like ransomware to the business.

Evolving BCDR Needs Paving Way for New Age BCDR Features/Capabilities

Most of the companies today are realizing the importance of having BCDR solutions that can deal with attacks such as ransomware effectively. Organizations today are looking for BCDR solutions that are both efficient as well as feature rich. When we asked the CIO community as to what their expectations from new age BCDR solutions would be, they highlighted some of the important parameters.

WHAT ORGANIZATIONS LOOK FOR IN NEW AGE BCDR SOLUTION?

- **35%** DR Mechanisms available
- **39%** Scalability & Elasticity Offered
- **42%** Availability Offered
- **47%** Security Features Integrated
- **49%** Recovery & restoration Time Committed

Sensing the changing requirements of businesses, BCDR solution providers are coming up with new features and capabilities that can make these backup and recovery solutions much more efficient and effective in fighting attacks like ransomware. In recent times, BCDR solutions that can effectively complement the existing IT security solutions is becoming a priority for organizations. BCDR solution providers too are coming up with new features/capabilities that are developed keeping in mind the evolving nature of ransomware attacks and the increasing importance of efficient and effective backup and recovery solution.

BCDR solution providers are coming up with enhanced recovery capabilities where critical workloads instantly get recovered whenever there is an attack. The recovery process happens from different means like storage snapshots and replicas. Today's BCDR solutions are also enabling backup anywhere capabilities where organizations have the liberty to backup their critical infrastructure from on-premise environment to cloud or from cloud to on-premise or from cloud to cloud. This enables organizations to prepare for every situation irrespective of where the data resides. Solution providers are also including immutable backup capabilities where backups happen right at the storage level which can be direct-to-object storage and provides insights on whether the backup has actually happened or not. In addition to this, the continuous monitoring capabilities with proactive alerts and real-time visibility and active monitoring makes BCDR more efficient. The automated testing and recovery process again enables organizations to monitor the quality of backups at regular intervals.

WHAT NEW AGE BCDR SOLUTIONS OFFER?

Enhanced Recovery Capabilities
Critical workloads Instant Recovery; Recovery from Storage Snapshots and

"Backup Anywhere" Capabilities
Backup from on-premise to cloud; cloud to on-premise & cloud to cloud

Immutable Backup
Storage layer level immutability; direct-to-object storage; Insights ensuring data protection

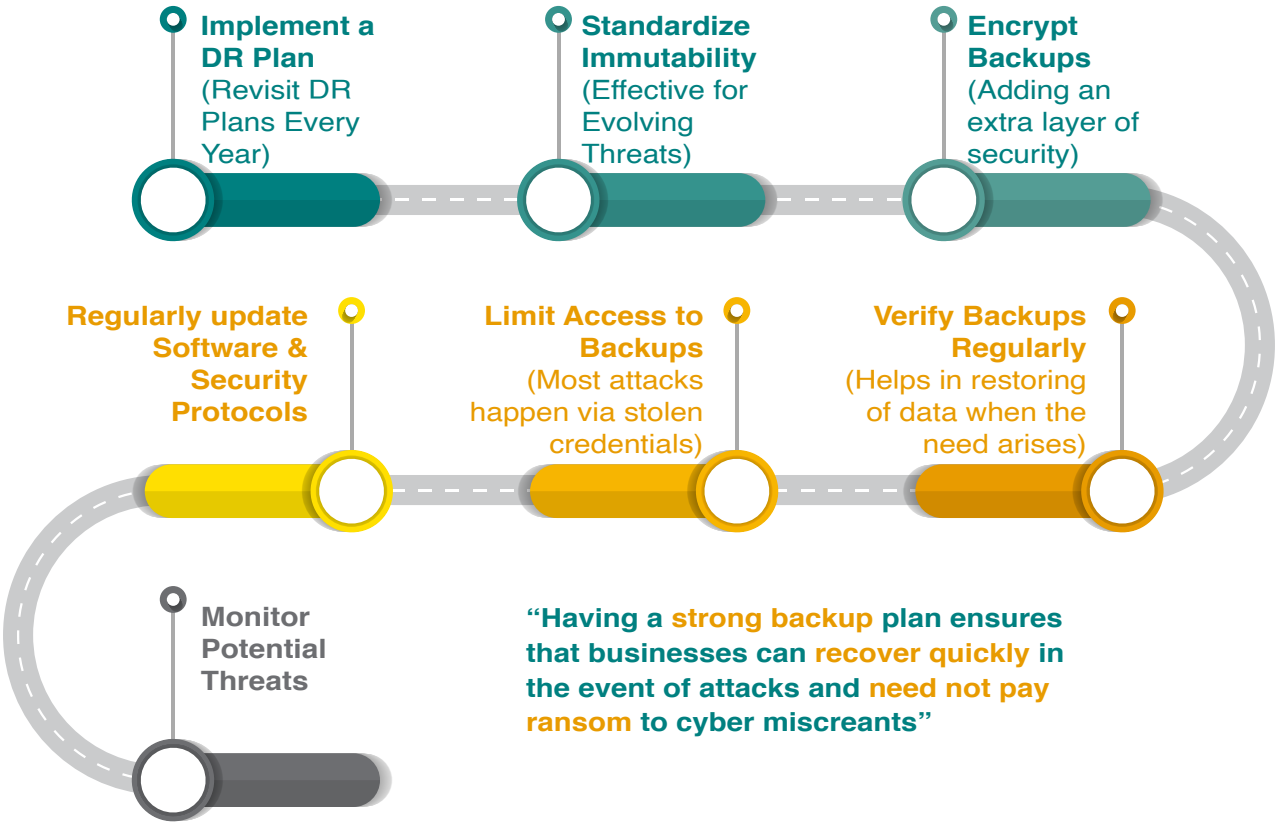
Continuous Monitoring Capabilities
Proactive alerts, real time visibility, active monitoring of recovery resources

Automated Testing and Recovery
RTO, RPO Adherence; automated recovery verification; real-time documentation of testing & failover plans

Best Practices that make BCDR fight Ransomware Attacks

As businesses continue to increase their data dependency, the need for effective BCDR based solutions continue to grow. As a result, companies today are in need of establishing a standard best practice that can help them in keeping attacks like ransomware away. Some of the key points that organizations need to consider when developing an effective BCDR setup includes,

ATTACKERS CATEGORICALLY TARGET "BACKUP INFRASTRUCTURE" AS BACKUP IS A CRITICAL INFRASTRUCTURE FOR BUSINESS CONTINUITY



"Having a strong backup plan ensures that businesses can recover quickly in the event of attacks and need not pay ransom to cyber miscreants"

Companies are realizing the importance of having a strong backup and recovery mechanism in place. They are also aware that having just a BCDR plan will not suffice. For a BCDR solution to be effective, companies essentially need to align their cyber security measures with their BCDR strategy. By doing so, organizations create a standard best practice that can activate backup plan in case an attack happens and at the same time develop policies and processes that has the potential of preventing attacks from happening.

ABOUT VEEAM SOFTWARE

Veeam® is the leader in Modern Data Protection. The company provides backup, recovery and data management solutions through a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected from ransomware, disaster and harmful actors and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects 450,000 customers worldwide, including 81% of the Fortune 500 and 70% of the Global 2,000. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers and alliance partners. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @Veeam-Software and Twitter @Veeam.

ABOUT THINK TEAL

Think Teal is an Analyst firm tracking the Enterprise ICT Market in India. Think Teal helps technology firms understand the markets that they serve and support them in achieving their business objectives.

To understand more about Think Teal, reach out at connect@think-teal.com