ULTRA SECURE BACKUP

WHITEPAPER

Rethinking Backups

Why Backup Systems Are Now An Essential Part Of Security Operations.

13% increase in ransomware attacks in the last year

The most recent Verizon Data Breach Investigations Report (DBIR) found that ransomware attacks increased by 13% in the last year. This increase is steeper than the combined growth in attacks in the previous five years. The report analyzed over 24,000 security incidents, of which 5,212 were proven data breaches. Accenture estimated last year that a ransomware attack is taking place approximately every 11 seconds.

The impact of this meteoric rise in attacks has been palpable. Organizations are now spending more money than ever on cybersecurity. Gartner estimates the total expenditure on information security will reach $172 billion in 2022. This expenditure is hardly good news for CISOs, though. In a tight market, security teams will likely be expected to deliver more value per dollar invested. Even more sobering is the estimate that this spending could go up to $1.75 trillion by 2025.

Why did ransomware attacks become so ubiquitous? Why did criminals switch from low-profile data theft to all-out, headline-grabbing attacks such as the Colonial Pipeline attack? And what are the security implications?

Not just data – Company operations are at risk

High-profile cyber-attacks impact the 'real' economy, critical utilities, and disruption, if not loss of civilian lives. With the growing scale of the impact comes greater scrutiny and systemic repercussions. The 2021 Colonial Pipeline attack prompted the Cybersecurity and Infrastructure Security Agency (CISA) to create a Joint Ransomware Task Force. The Department of Justice (DoJ) is to launch separate international initiatives to track illegal cryptocurrency transfers to try and prevent the most virulent threat actors. The banking sanctions currently imposed on Russia have also apparently hurt the ability of attackers to access the requisite Internet facilities (such as contacting and paying initial access brokers, crypters, and hosting service providers) or even get the payout from successful attacks. And yet, the cybercrime market share of ransomware attacks continues to grow.

The Verizon report opines that ransomware attacks are still one of the most effective means for threat actors to access and monetize private information illegally. Also, companies valorized data protection so much that we got really good at protecting user data such as PII and financial information with encryption and best practices. This compelled attackers to turn to a threat mechanism that increased the threat level manifold – not just reputational damage from a breach but actual stoppage of all operations. A recent example of this is the attack on Sunwing Vacations data provider – this attack ceased all flight operations and severely damaged Sunwing's reputation. This is no longer a security issue. It's a full-fledged disaster.

Whether we like it or not, disaster scenarios will be more common going forward – even as organizations try to beef up security defenses against data breaches. The old approach of safeguarding data at all costs will not cut it. Companies can no longer afford to treat security and disaster recovery/ backup as separate domains.

Blurring lines between backup and security – Backups are now a security concern

Traditionally, backup architects have been concerned with file deletions, server crashes, flooded server rooms, and website shutdowns. Unfortunately, we've not been very good with it, as complete disaster recovery scenarios are not tested very often. Their performance was typically based on RTO and RPO metrics (how quickly they can recover, the amount of data they recover, etc.) vis-à-vis the cost of backup software and storage or ROI. On the other hand, security teams focus on securing sensitive data and preventing unauthorized access and breaches. As disaster recovery has become a pressing need, most companies find themselves unprepared. The cost of all those untested DR scenarios is starting to add up.

Attackers are wise to the act. They have now started to attack the backups directly. Malware is now deeply embedded in backups, and hackers will wait weeks or months before activating them to secure the Attack-LoopTM. Their payouts are secured if they can prevent the company from recovering data, their payouts are secured.

Disk, tape, or even cloud backups are often incapable of guaranteeing uptime in cases where you are infected with ransomware or another virus, server or network failure, or your facility is temporarily shut down. Recent data shows us that disk and tape backups fail anywhere from 20% to 40% of the time during restoration and are not regularly tested or validated. Cloud backup can take days or weeks to recover data depending on the amount of data stored and your bandwidth. Organizations that have traditionally focused on backup-only solutions often don't realize until it is too late that the protection does not extend to more than their data. Your mission-critical applications, server, and network are not backed up effectively, preventing access to your data and files.

Organizations need to shift their focus from looking at backups in isolation and consider recoverability and business continuity as an integral part of their security suite. An inadequate or incomplete solution could put your entire organization at risk of maintaining a stable and profitable operational environment.

How CISOs (Chief Information Security Officers) need to rethink backups

As backup needs have become a priority, most CISOs are starting to realize that they need to have a lot more oversight into how backups work, what backup tools are being used, how secure these tools are, and ensuring the regular testing of restores and DR scenarios.

Your backup infrastructure should match your needs. If you are concerned about the possibility of hardware failure or natural disasters, then you will want to consider off-site backup solutions. However, if you are more concerned with being locked out of data on site, then other strategies come to mind. Air-gapped backups and immutable backups are popular right now, but these, too, are easily subverted by attackers. Your backup protection strategy needs to adapt and advance along with changes in tactics by attackers. Having software that can hunt and kill ransomware malware before data is backed up or restored is critical. And ensuring that attackers can't access the backup software or data sets to damage backups is even more important.

As the ability to harness data becomes the primary competitive differentiator between businesses and big data becomes a necessity, your recoverability and backup solutions must be able to scale their ability to protect data adaptively. You also need to have a process wherein new servers, applications, and data stores are added to the backup process seamlessly.

To adopt security best practices that are best suited to your organization, you need to consider the following aspects:

- *Has my company ever been hacked before?*
- *Are careless employees a concern when it comes to security?*
- *Is my location at risk for weather-related damage such as flooding or wildfires?*
- *Do clients log in remotely to my system to access data or services?*

Most importantly, companies need to have a system for maintaining data about recent incidents. It means having an efficient process in systems organization and incident documentation. An Information Officer reviewing data should glean what happened in the past, what the threat was, and the steps needed to avoid such instances in the future.

Who in your organization should be involved in backup architecture decisions?

- It's no longer an infrastructure only decision.
- Needs to involve CSO/CISO, CIO, Cloud Architects, Backup Architects, Disaster Recovery/Business Continuity personnel.
- It's a multi-disciplinary team that needs to understand how data can be attacked and their options to protect it. The shift of focus towards SMBs, healthcare and public departments

Following the altered approach toward backups, architectural decisions about backups should no longer be an infrastructure-only decisions. Backup decisions need to move beyond RTOs and RPOs to address broader organizational needs in recovery. It needs to become a more holistic decision-making process involving the CISO, CIO, cloud architects, backup architects, and teams responsible for disaster recovery and business continuity. To build a holistic approach toward disaster recovery, organizations must put in place a multi-disciplinary team that understands how data can be targeted in diverse ways. The diverse backgrounds will help paint a complete picture of your recovery needs than having your backup architects work in isolation. Based on this information, you can take stock and review your options for safer backups and data management.

Essential guidance – What to do next

- Run “What If” ransomware fire drills
- Set up a working committee between CSO and CIO to start your review process.

The immediate steps would be to review all existing backup and recovery processes. The best way to do that would be to set up a working committee between your CSO and CIO to initiate the review process. It would be a good idea to run through simulation exercises based on ‘what if’ scenarios. This might include examples such as:

- What if your backups are corrupted?
- What if your backups going back 3 months are infected with malware?
- What if your admin credentials have been compromised?

Your strategies in responding to each of these scenarios might differ, but your preparedness will ultimately affect the outcome of your disaster recovery process. The more prepared you are with thoroughly tested DR scenarios, the better your chances are of successfully preventing work stoppages, prolonged downtimes, and even increasing resilience to cyber-attacks throughout your organization.

Rethinking your backup processes can help your company avoid big losses in the long run from ransomware and various other evolving threats. Remember that these threats will continue to attack not just your data but the integrity of your entire operations by targeting your backups. It is high time for us to move beyond perceiving backups in isolation and treating them as an integral component of any disaster recovery scenario. Asigra’s purpose-made backup & recovery solution to combat Ransomware 3.0 could help your company meet your security & recovery needs now and well into the future.

Next Steps

Organizations are now spending more than ever on cybersecurity. Learn why here & how rethinking backups can help. Contact Asigra today!

Contact Us