arkphire
a Presidio Company

PRESIDIO®

rubrik

SIMPLE CYBERSECURITY TIPS FOR SAVVY CIOS

THE FOUR IMMUTABLE LAWS

OF PROTECTING DATA IN THE CLOUD

WRITTEN BY: RAPHAEL MEYEROWITZ

THE FOUR IMMUTABLE LAWS

OF PROTECTING DATA IN THE CLOUD

SIMPLE CYBERSECURITY TIPS FOR SAVVY CIOS

If data is the lifeblood of an organization, then securing it is more critical than ever–especially through complexities introduced with hybrid and multi clouds. Following these four truths can keep your business functioning well.

1 Backup and recovery of your data in the public cloud is YOUR responsibility.

2 Your data in the public cloud is NOT PROTECTED from ransomware.

3 Your backup and recovery solution should support your public cloud environment and your applications.

4 Backup and recovery should be part of a larger organizational data protection vision and strategy.

PRESIDIO®

rubrik

IMMUTABLE LAW #1

BACKUP AND RECOVERY OF YOUR DATA IN THE PUBLIC CLOUD IS **YOUR** RESPONSIBILITY.

Many IT leaders believe that when they migrate applications to the public cloud, backup of their data is covered. This is an unfortunate and common misconception.

AWS, Azure and Google clearly state that the responsibility lies with the client. Organizations that believe the cloud service is their backup can suffer loss from deletion, security incidents, software bugs and ransomware attacks. Of course, the worst-case scenario is a sudden, irreversible and permanent loss of their data. To avoid any of those unfortunate events, it is essential to store a copy of your data on a separate platform, and to make copies of your data on a consistent and regular basis.

Backup in the cloud can be extremely different from traditional approaches of backing up physical or virtual machines. The good news is that fantastic solutions are available to help you protect your data in the cloud from a variety of threats.

54%

Increase in downtime costs from 2018 to 2019. It is taking organizations longer to recover.[1]

5-10X

Costs in downtime following a ransomware attack can be five to 10 times the actual ransom amount.[2]

IMMUTABLE LAW #2

YOUR DATA IN THE PUBLIC CLOUD IS **NOT PROTECTED** FROM RANSOMWARE.

Once again, a tragic misconception is causing major harm to numerous organizations in all industries. Many incorrectly believe that data in the public cloud is secure from ransomware. Companies have had tremendous outages because they have not protected their data, especially their backups, after moving workloads to the cloud. **Your backup is your last chance to minimize disruption as a result of ransomware, so losing it can be disastrous.**

> ***Ransomware*** *refers to cyberattacks where an organization's mission-critical data is encrypted by attackers who then demand large ransom payments for the key to decrypt it so business can resume.*

The explosion of ransomware attacks has organizations rightfully concerned. Many of them have made funding available to defend against these attacks, while other important initiatives may not be provided with necessary funding as easily.

One way to make optimal use of your IT spend is to kill two birds with one stone. For example, solutions that help you avoid damage from ransomware attacks may be able to help you advance your cloud and data journey–like Rubrik, which gives you the ability to better manage your data from a single management plane.

> "Ransomware is rapidly shaping up to be the defining online security issue of our era."[3]
>
> *~ Steve Ranger at zdnet.com*

715%

Ransomware attacks have risen as much as 715% over 2019[4]

EXAMPLE: GARMIN

July 2020: Ransomware attack takes well-known GPS and aviation tech specialists entirely offline for more than 3 days.[5]

$10M

ransom + recovery

Evil Corp ransomware—a Russian cybercriminal gang

HOW TO AVOID BEING HURT BY RANSOMWARE

First, make sure you have an immutable backup solution in place.

Immutable backup means that your backup data cannot be read, modified or deleted by anyone. Only an application can read the backup copy. Effectively, no security exposure can tamper with your backups. Even if ransomware successfully encrypts data from other places, your backup data can be restored so you can avoid paying the ransom.

What is Immutable Backup and Why Is It Important?

Immutable backup means that once data has been written, it cannot be read, modified or deleted by any users on the company's network. Think of it as a backup copy that exists and no one can actually modify it. Only an application can read an immutable backup. This is key when it comes to cybersecurity, because essentially it means that nobody can tamper with your backup.

Secondly, set up your backup infrastructure on separate authentication domains.

That means that ransomware cannot get over to the backup domain because there are not credentials for it to log on. This independence ensures that you won't get locked out of your backup, and can get back up and running quickly in the event of an attack.

RANSOMWARE IN 2019-2020[6,1]

TOP 5

World Economic Forum Global Risks Report 2019 ranks cyberattacks among the TOP 5 global risks.[6]

82%

reported experiencing a disruptive event in the last 12 months (up from 76% in 2018).[1]

69%

lack confidence that they will be able to recover all their data following a cyberattack.[1]

IMMUTABLE LAW #3

YOUR BACKUP AND RECOVERY SOLUTION SHOULD SUPPORT YOUR PUBLIC CLOUD ENVIRONMENT AND YOUR APPLICATIONS.

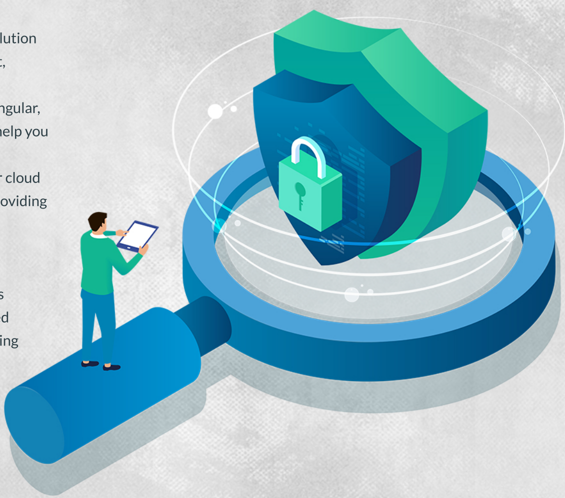
rubrik

Rubrik's solution provides tremendous advantages and can help you:

- Simplify and streamline your policy management
- Get rapid restores in just a few clicks
- Unify across hybrid and multiple clouds

Optimally, a cloud native data protection solution will help you automatically discover, protect, organize, and manage all your data and applications on multiple clouds through a singular, easy-to-use view. This type of solution will help you avoid having two different kinds of backup. Instead, it will be an extension, keeping your cloud data safe, enhancing data availability and providing greater resilience and recovery confidence.

It is important to develop a vision for your organization's data protection and a process to get from where you are to where you need to be. That process should include architecting backup and recovery solutions when you move workloads into the public cloud.



IMMUTABLE LAW #4

BACKUP AND RECOVERY SHOULD BE PART OF A LARGER ORGANIZATIONAL DATA PROTECTION VISION AND STRATEGY.

Clearly, backup and recovery is only one part of a larger strategy that now encompasses data wherever it resides, including hybrid and multi-cloud. Backup solutions can only be as effective as the data protection strategy they support.

Organizations will be best served when data protection is tied to a larger cloud strategy. Many companies have a “cloud-first” strategy. However, you may want to consider a “cloud-right” strategy that uses the right element of hybrid cloud for various workloads based on several factors—from cost and compliance to data sensitivity and users’ need for access to it.

Make sure you develop a strong vision and an effective strategy for your data protection that meets your business needs, complete with a process that best gets you there incorporating the most impactful solutions.

PRESIDIO®

Presidio was recently engaged by a large retailer with 700 physical stores and an aggressive public cloud migration journey, fueled further by the pandemic. The retailer was especially concerned about ransomware attacks as its backup solution that had failed DR tests. We built out a strategy supported by an immutable file system with Rubrik, replicating one site to another and reducing risk and downtime for the organization, which now does not have to worry about ransomware attacks–and has better access to data and ability to mine it for insights to grow their business.

rubrik

arkphire
a Presidio Company

PRESIDIO®

rubrik

SIMPLE CYBERSECURITY TIPS FOR SAVVY CIOS

THE FOUR IMMUTABLE LAWS

OF PROTECTING DATA IN THE CLOUD

RAPHAEL MEYEROWITZ
Vice President, Office of the CTO at Presidio

With more than 15 years of experience in information technology, he has contributed significantly to technology-business goals for a number of companies. With a strong background in managing projects, people, and processes, he excels at identifying pain points and areas for improvement, creating the appropriate technology strategies, and driving implementation of solutions that yield outstanding results.

[1] Data Protection Index 2020 • [2] https://searchsecurity.techtarget.com/news/252489235/Gartner-Paying-after-ransomware-attacks-carries-big-risks • [3] https://www.zdnet.com/article/ransomware-is-now-your-biggest-online-security-nightmare-and-its-about-to-get-worse/
[4] www.zdnet.com/article/ransomware-huge-rise-in-attacks-this-year-as-cyber-criminals-hunt-bigger-pay-days/ • [5] https://threatpost.com/garmin-pays-evil-corp-ransomware-attack-reports/157971/ • [6] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf