The
Broadcasters' Desktop Resource
www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Bits and Bytes

World Backup Day – A Good Reminder!

By Barry Mishkind

[March 2022] Are you a professional procrastinator? All kidding aside, we all know the reasons why we should regularly backup our computers and key files. Yet, the reality is that everyday issues often take over the day, and we basically end up saying "I'll get to it tomorrow." But that could leave you open for a nasty surprise/problems.

Thursday, March 31 is World Backup Day, the day this year especially intended to focus attention so business – and personal users – will take a moment to remember why backups are so important.

We tend to expect that whenever we open our computers, everything will be there – our applications, especially the "mission critical ones," our data, and all the various utilities we depend upon at work, and at home. Yet, there are many things that can rob us of days, weeks, even years of work.

Simple equipment failures like a hard drive dying, various disasters ranging from lightning strikes to fires to floods, and more recently, malware and ransomware from bad actors all combine

So, World Backup Day is a good opportunity to consider just what would happen if you lost access to your files.

THE WILD WEST

It does not take a lot of effort to know ransomware has become such a huge threat to private businesses and government agencies around the world.

A key reason backup has risen to the top of most IT professionals' priority list is the number and level of attacks that are increasing. Just this week, the US Government issued a statement warning businesses, especially broadcasters that hackers from Russia are targeting US businesses.

Could this affect you?

Aside from the high-profile attacks that sometimes turn up in the new, including Colonial Pipeline, JBS, Garmin, and Acer, many people now personally know a colleague whose business was attacked. While ransomware was thought to be only a problem for large enterprise organizations, some may be surprised to learn that according to recent research, such as that from Coveware, most targets now include small and medium businesses.

In fact, Coveware has indicated that 72% of targeted businesses have fewer than 1,000 employees, and 37% have fewer than 100. Organizations are projected to have paid out $20B in 2021, a 100% year-on-

year increase for the last four years – and it is only going to get worse with new business models like RaaS (Ransomware as a Service) making ransomware easier and more accessible than ever.

Which brings us back to why it is more important than ever to backup your data!

VOICES OF REASON

Major IT company executives emphasize that regular backups need to be done regularly, especially for "mission critical" applications such as the program automation and bookkeeping that drives broadcasting.

Don Boxley, CEO and Co-Founder, DH2i (www.dh2i.com) says few would disagree that backing up data is one of the most critical protections that an organization can implement to help ensure the ability to recover and maintain operations in the event of a failure, disaster or malware attack - such as ransomware. Nevertheless, he notes research has shown that while almost 90% of organizations are backing up, only about 41% backup daily, leading to a high number of companies admitting that they have had data loss events that have resulted in downtime.

Boxley says "On World Backup Day, I would encourage organizations to take a hard look at backup as well as all policies, procedures and technology they have in place to ensure high availability (HA) and disaster resilience. And then, I would recommend they evaluate if they were to experience a failure, disaster or cyber-attack, how quickly could they recover, and would be able to weather that downtime from a business, legal and/or regulations compliance standpoint. It is well stated that an ounce of prevention is worth a pound of cure."

BACKUP TO AVOID DISRUPTION AND ECONOMIC LOSS

Not long ago, a major US broadcast company was essentially shut down for over a week, as they tried to recover from a ransomware attack. The lost revenue as well as the inability of staff to work normally was tremendous.

The CTO of StorCentric (www.storcentric.com), Surya Varanasi comments that "on World Backup Day, we are reminded that ransomware and other types of malicious malware can disrupt any environment. And further, while hundreds of thousands if not millions might be at stake for the actual ransom payment, the gravest consequences of ransomware is data loss and downtime."

Varanasi says "Today, the process of backing up has become highly automated. But now, as ransomware and other malware attacks continue to increase in severity and sophistication, we understand the need to protect backed up data by making it immutable and by eliminating any way that data can be deleted or corrupted."

This extra step might be a basic but highly effective protection against hackers.

"An Unbreakable Backup does exactly that by creating an immutable, object-locked format, and then takes it a step further by storing the admin keys in another location entirely for added protection," he says.

"Other key capabilities users should look for include policy-driven data integrity checks that can scrub the data for faults, and auto-heals without any user intervention," he said, recommending IT systems

employ dual controllers and RAID-based protection that can provide data access in the event of component failure.

Using such a RAID system is good, Varanasi says: “Recovery of data will also be faster because RAID-protected disk arrays are able to read faster than they can write. With an Unbreakable Backup solution that encompasses these capabilities, users can ease their worry about their ability to recover and redirect their time and attention to activities that more directly impact the organization’s bottom-line objectives.”

PLANNING AHEAD IS SMART

Not if, but it is a given that at some point most will suffer a failure, disaster or cyber-attack, according to JG Heithcock, GM, Retrospect, a StorCentric Company (www.retrospect.com):

The key is planning, understand the best way to recover should a severe problem happens. Heithcock says that “given the world’s economic and political climate, the customers I speak with are most concerned about their ability to detect and recover from a malicious ransomware attack.

“My advice to these customers is that beyond protection, organizations must be able to detect ransomware as early as possible to stop the threat and ensure their ability to remediate and recover. A backup solution that includes anomaly detection to identify changes in an environment that warrants the attention of IT is a must. … And, those anomalies must be immediately reported to management, as well as aggregated for future ML/analyzing purposes.”

As others have said, just detecting an intrusion (successful or not) is not enough.

“Of course, the next step after detecting the anomaly is providing the ability to recover in the event of a successful ransomware attack,” Heaithcock notes. “This is best accomplished with an immutable backup copy of data (a.k.a., object locking) which makes certain that the data backup cannot be altered or changed in any way.”

We hope you do take the time to use the World Backup Day as intended: a time to stop and evaluate just where you would be without your computer system – and set up so you will not be added to the list of companies that lost time, work product, or large amounts of money.

- - -

Did you enjoy this article? Would you like to know when more articles like this are posted? It only takes 30 seconds to sign up here for the one-time-a-week BDR Newsletter.

- - -

Return to The BDR Menu