PRIANTO

UNITRENDS

# WHY BACKUP IS THE LAST LINE OF DEFENSE AGAINST RANSOMWARE AND CYBERCRIME

# Introduction

Cybercrime and the scourge of ransomware break through the best defenses, even those with layered security in place. Hackers are often after your data, corrupting it through viruses and malware, and locking it up for payment through ransomware.

Your layered security service offering is not complete unless you can take the last stand by protecting data with quickly available, full, uncorrupted copies of everything your business depends on to avoid crippling downtime.

Your business might have some form of backup, and if not, it is something you should clearly rectify. However, backup does not mean data is fully protected. Disk and tape backups are prone to failure during recovery. In addition, Windows-based backup appliances and software are susceptible to ransomware attacks. Simply put, backup is not a guarantee against data loss.

**Mike Sanders, CEO of Unitrends**, has helped thousands of businesses fully and completely protect their data for years. He understands why backup is truly the last line of defense and how IT professionals should best protect businesses from the unfortunate reality of cybercrime. This whitepaper reflects the insights Sanders developed from years of backup experience.


© 2020 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

## Why is Cybercrime so Awful?

**A recent ZDNet study of over 2,600 senior leaders ranked information theft as the most expensive and fastest rising consequence of cybercrime.[1]**

**Cybercrime is the fastest growing form of organized crime, and it is already, stunningly, larger than any other form of organized crime. Think about that for a minute. At over $3 trillion a year, cybercrime is bigger than all of the cocaine, heroin and marijuana business combined.[2]**

Why does this matter? Despite having antivirus and anti-malware tools, firewalls and other protections, cybercrime, ransomware and malware still get through.

How does this happen? Cybercrime is a business. For every person writing code to stop attacks, there are myriad others, including highly organized development teams and state-sponsored groups, doing the exact opposite. These cybercriminals are making billions of dollars in revenue, and there is not much law enforcement can do about it.

**Whether you know it or not, your business desperately needs the true data protection that top-shelf backup endemic to business continuity disaster recovery (BCDR) solutions provide. It's alarming to know that 75 percent of SMBs do not have a disaster recovery plan or true solution in place.[3]**

When ransomware hits, these SMBs have little choice but to pay up.

**SMBs are the sweet spot for ransomware attacks since smaller shops generally do not have rich defenses or full available backups of their data. In fact, sophisticated ransomware attacks like Ryuk attack SMBs since they are easy targets. This can potentially cost the U.S. economy more than $7.5 billion.[4]**

What can SMBs do to stave off ransomware? Simple. They need a backup solution that is robust enough to secure and preserve data and restore it quickly if any data is encrypted. An even more effective defense will detect ransomware before it takes hold.

But isn't all backup the same?

Not all backup is created equal. To demonstrate, let's consider how different approaches cope, or fail to cope, with recovering from a ransomware attack. After all, the real value of any backup solution is in the recovery.

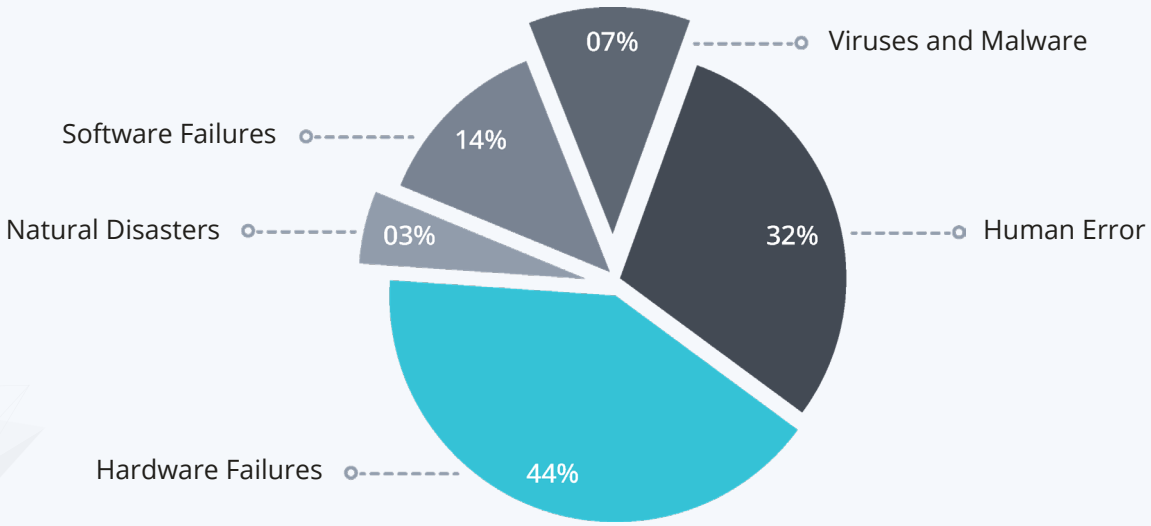

© 2020 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

# Direct to Cloud

The benefits of direct-to-cloud backup are that it is easy and inexpensive. The downside is that in the event of a ransomware attack, your business operations go down for a long time. Imagine having 15 employees on-site and each machine has 100 GB. That is 1.5TB, plus another 1.5TB for their services. That's 3TB altogether. Your business probably has a 200 Mb/s pipe to serve those workers.

If you devote 100 percent of that bandwidth for the entire time needed to do the recovery, you are looking at a 15-day process to bring back the data. That can cripple your SMB. There are many causes of data loss as you can see in Figure 1, including viruses/malware, software failure, hardware failures (the leading cause), human error, and finally natural disasters – which account for only 3 percent of major outages or data loss.

FIGURE 1
DATA LOSS CULPRITS




**Sources:** Backup and Recovery Solutions Review and Baseline Data Services

**Tragically, a natural disaster is the only circumstance well served by a direct-to-cloud-only strategy.**


© 2020 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

## Backup to a NAS

Many SMBs think their bases are covered by backing up to a networked-attached storage (NAS) device. NAS devices offer far faster data recovery than the cloud, but they are still deficient in several critical ways. First, you have to perform a full server recovery before you can spin the servers back up. That takes time, and as desktops struggle to come back up, data access is down until the servers are fully operable.

The bigger issue is being confident of a successful recovery. It is incredibly difficult and expensive to do automated recovery testing on these backups, and without the confidence such testing provides, many SMBs pay up rather than go through their untested, and in many cases poorly designed, recovery plans.

**Too many SMBs are indeed caught flat-footed. A survey conducted by the research firm Clutch found that over 60 percent of SMBs that suffered a major data loss event said that their business continuity and disaster recovery (BCDR) plan was nowhere near as effective as they expected.**[5]

## Enterprise-Class BCDR – The Unitrends Answer

The Unitrends approach is a completely different story. It is not just backup and recovery, but true BCDR. It does this with a combination of on-premises appliances and the cloud – thus offering the best of both worlds. This all-in-one BCDR solution does not require the stitching together of disparate vendor tools. Unitrends technology has a proven track record over the years for SMB and enterprise use.

Meanwhile, the Unitrends all-in-one solution comes with all-in-one monthly pricing that covers everything – including the ability to easily and affordably scale. This means you can adjust capacity as your needs increase or shrink (along with costs).

Unitrends offers true and fast recovery from disaster, and with this speed also provides true business continuity. Moreover, your business data is ransomware-proof.

However, the real key is that with Unitrends you can automate the testing, so you KNOW your recovery will work. It also allows you to apply those same processes used while testing to failover in the event of data loss.

It is this type of system that makes a Ryuk ransomware attack a near non-event for most businesses.

## The Unitrends Story

Unitrends is a wholly owned subsidiary of Kaseya. Unitrends is an enterprise-class BCDR solution provider that has been in business for over 30 years with over 30,000 customers.

Unitrends increases uptime and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a “one throat to choke” set of offerings that allow our customers to focus on their business rather than backup.

Get an in-depth demo of Unitrends today.


© 2020 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

## Sources


1. Cybercrime is increasing and more costly for organizations, ZDNet
2. Cybercrime Damages $6 Trillion By 2021, Cybercrime Magazine
3. Why You Must Know this Number to Keep Your Business Up and Running, Eguardtech
4. The 10 Biggest Ransomware Attacks of 2019, CRN Magazine
5. Don't let a Data Loss Nightmare Become Your Reality, Unitrends MSP


## Reach Out Today!


Your Unitrends Experts:
Alan Fink at Prianto Distribution
alan.fink@prianto.com
01635 225 262

Paul Hollow at Unitrends
phollow@unitrends.com
0203 608 2749


## ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY

© 2020 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

PART #WP-2104-ENG-A