

eBook

Financial Services Firm?

Add Business Continuity to your Bottom Line

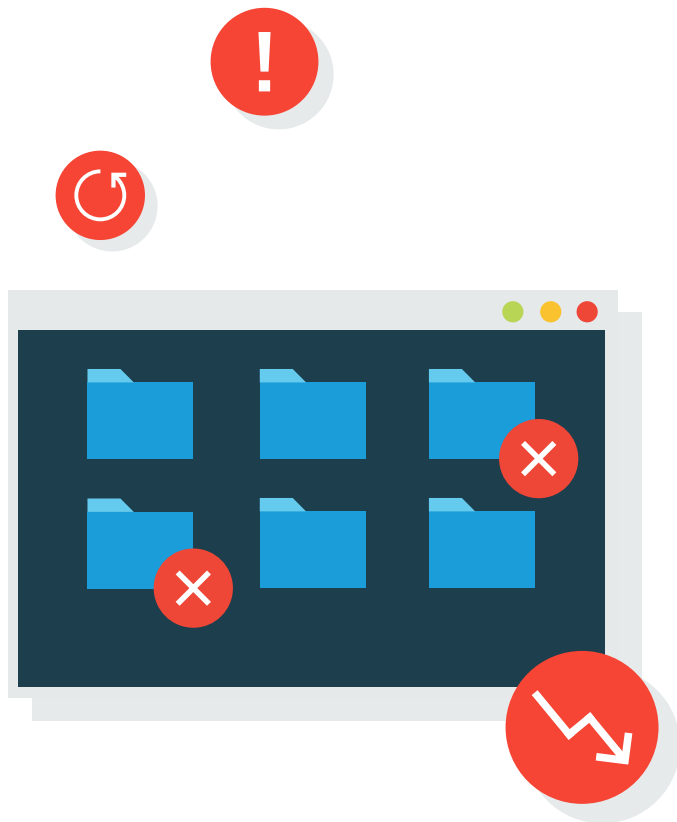


Introduction

As a financial services firm, your clients depend on your guidance to help them make the most out of their fiscal decisions. From accounting to hedge fund management, your clients gain peace of mind when advised properly. These relationships require trust, often built over time. What would happen if that trust were threatened? How long could you keep your clients at ease if they were unable to retrieve information or make withdrawals? What would happen if you couldn't get their tax returns filed in time? What would happen if someone's identity were stolen and you couldn't access their information to stop it?

In the financial industry, downtime can be detrimental to your ability to do your job. Nowadays, downtime threats are not only weather related. Entire systems can fall victim to ransomware. Individual identities can be stolen. In these instances, your clients will turn to you for financial security. Being able to deliver that service is crucial to your reputation and business' livelihood.

Entire systems can fall victim to ransomware. Individual identities can be stolen. In these instances, your clients will turn to you for financial security.



A False Sense of Security

While you may be taking some precautions, such as securing and backing up your sensitive data, sometimes that's not enough. There is a common misconception that data is safe if backed up once a day, but this outdated practice is no longer sufficient for several reasons:

- If you forget to perform the backup or the backup process fails, you're not protected.
- If you only back up your files once a day, you're left vulnerable to the loss of an entire day's work.
- If you don't properly validate your backup files, you could be in for an unpleasant surprise when you actually try to use those files to restore your company's operations.
- If you only back up your files on-site, you could lose them too—leaving you with no way to meet client requests.
- If you only back up your raw data, rather than all your application and server configuration files, it could take several days to restore your practice —because you will also have to rebuild your servers, operating systems, applications, etc.

Some financial services firms are turning to business interruption insurance to cover the costs to rebuild, restore, or regain lost income. However, while an insurance provider may write you a check for the cost of a server that gets damaged because of a broken pipe, it won't shield you from damaged or lost client relationships. Ultimately, your reputation isn't something for which you can easily be compensated.

How Vulnerable Are You?

If your company identifies as a business that doesn't have the IT resources to effectively recover from a major outage, make sure you're weighing all of the factors around the costs of downtime. Here are the facts:

- US businesses lose \$12 billion annually due to data loss.¹
- 93% of companies that lose their data center for 10+ days file for bankruptcy within one year.²

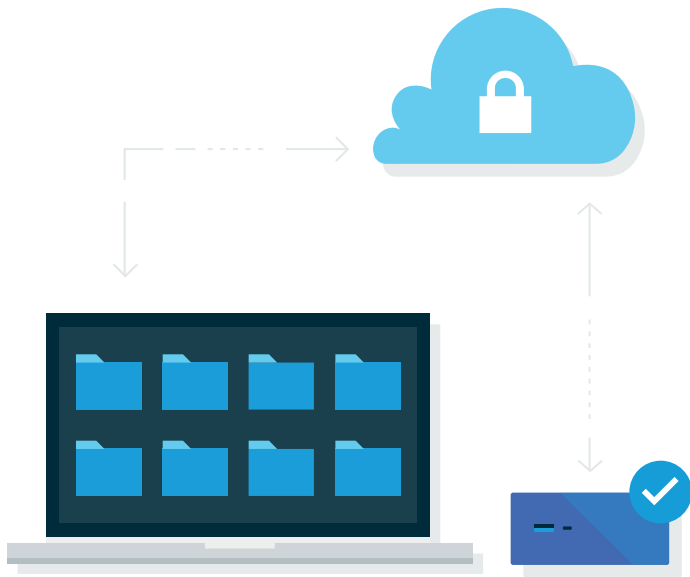
Best Practices for Financial Services IT

In a 2017 survey by the Depository Trust & Clearing Corporation, 78% of financial services firms reported cyber risk among their top five concerns³. Their concern seems justified as 2017 was a costly year for the financial services industry. The Ponemon Institute reported that the cost of cyber attacks in 2017 averaged to \$18.28 million per financial services company⁴. These costly incidents seem to be on the rise, but there are some precautions you can take to safeguard your data:

- Outsource your company's IT needs to an expert who has experience in the financial industry.
- Don't sacrifice quality to save money when purchasing hardware. It will benefit you (and your bottom line) to have strong technology in the long run.
- Perform timely hardware and software updates, maintenance and backups.
- Establish, review and maintain system security of all practice technology.

Any company that has not recently re-assessed its backup and disaster recovery procedures should therefore do so in order to conform to these industry-standard best practices.





A true business continuity solution will protect data on-premises and in the cloud.

For more information please contact:
David Gemma | CEO/CMO | Phone: 203.269.6111 |
Email: david.gemma@unapen.com | UNAPEN, Inc. |
<https://unapen.com>

Here's what one MSP had to say about the need for a strong business continuity solution in the financial industry:

"The big thing is that the decisions made in the financial services industry can result in millions of dollars of difference in one direction or another. If systems are down and they can't make a trade they've got a problem. If there's a hiccup or a problem, being able to failover gets companies up and running. Knowledge is power and the data that they have is their knowledge." -Paul Riedl, CEO, River Run Computers Inc.

The Better Way: Business Continuity

Business continuity describes a complete solution for backup and disaster recovery. A true business continuity solution will protect data on-premises and in the cloud. Whether data is on servers or in SaaS applications, it needs to be backed up. Business continuity goes a step further and offers you the ability to restore your data, which we call disaster recovery.

Whether a business is faced with a natural disaster, or one man-made, a strong solution will have you up and running in minutes. Solutions that leverage the hybrid cloud can guarantee a quicker restore time as well. Why? Local backups are great to keep data stored on local devices, but if something happens to that device, then what? A hybrid cloud backup solution takes an initial backup on a local device, and then replicates the backup to a cloud server. Cloud-only solutions are not as reliable on their own due to bandwidth issues. A hybrid model works to alleviate the vulnerabilities by implementing both processes to fill in the gaps. That's intelligent business continuity.