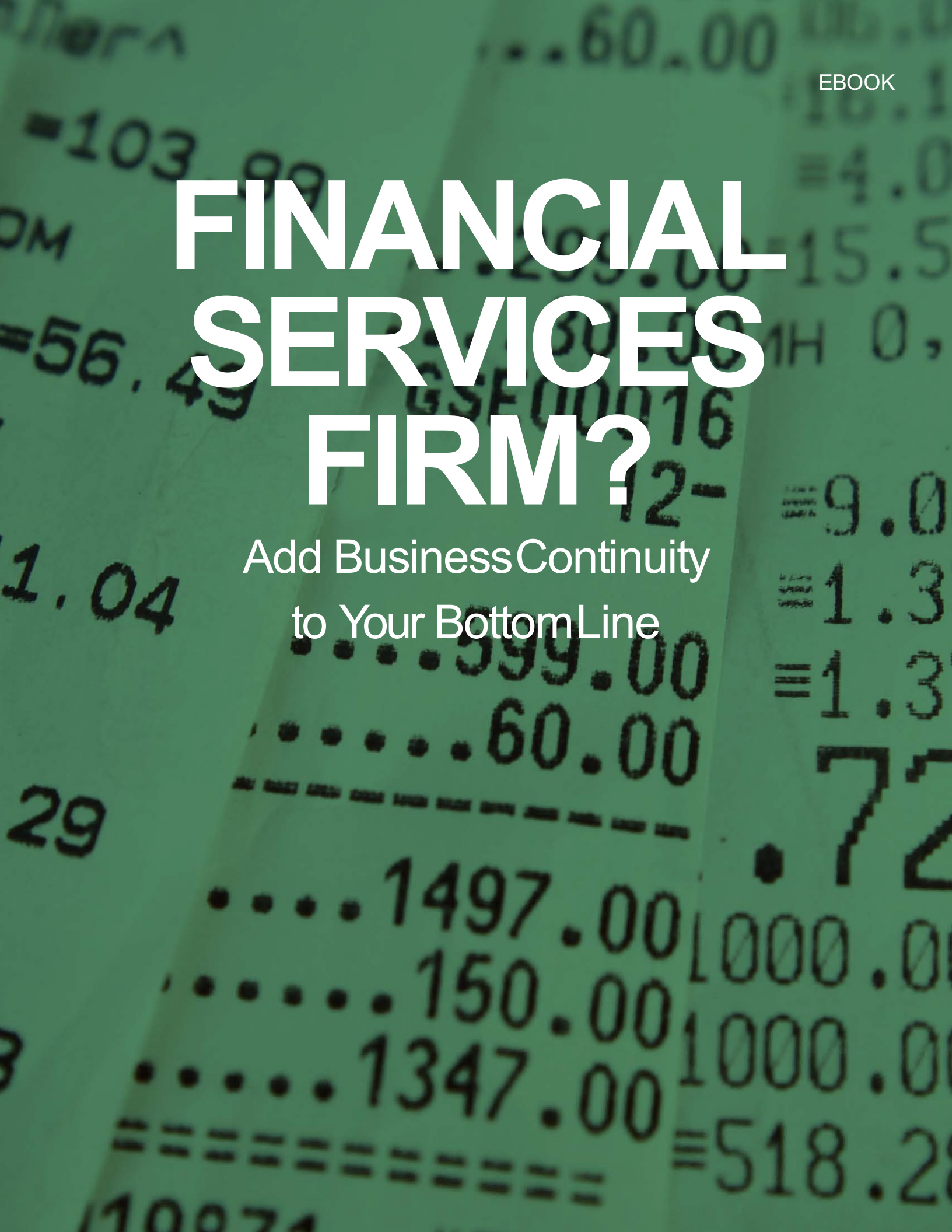
EBOOK

FINANCIAL SERVICES FIRM?

Add Business Continuity to Your Bottom Line



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?

For businesses in finance, 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 There is a common misconception that data is safe if backed up once a day, but this outdated practice is no longer sufficient for several reasons: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 2014 survey by the Depository Trust & Clearing Corporation, 84% of financial services firms reported cyber risk among their top five concerns3. Their concern seems justified as 2014 was a costly year for the financial services industry. The Ponemon Institute reported that the cost of cyber attacks in 2014 averaged to $20.8 million per financial services company.4 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 allpractice technology.

> **The cost of cyber attacks in 2014 averaged to $20.8 million per financial services company.**
>
> The Ponemon Institute

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.

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.

Business Continuity for Financial Services

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.

BINARYLOGIC

The Better Way with BinaryLogic Inc.

BinaryLogic offers a superior solution for safeguarding the day-to-day wellness of your business. Automatically backing up both your practice data and your server/application configuration files for you continuously throughout the day—storing them on both a device in your office and in the cloud. BinaryLogic also continuously validates the integrity of your data and configuration files to ensure your backups are functional and have not been corrupted by a virus or other malware.

In the event that your office experiences a hardware failure, extreme weather event, or any other calamity, the solutions deployed by BinaryLogic help by enabling you to keep running your practice from either your local backup device or your cloud files.

Advantages of BinaryLogic support include:

- All backups are performed automatically and reliably for you.
- You can have full confidence in your ability to recover from any sort disaster.
- You can restore your practice operations quickly with a single phone call to BinaryLogic

Have confidence that your practice is protected against any outage resulting from a disaster. You won't have to worry about the potential financial consequences of such a disaster—and neither will your clients.

It's time to safeguard the credibility of your practice the same way you safeguard the credibility of your clients. Call BinaryLogic today at 780-665-6677 for a free assessment, no-obligation assessment of your practice's backup and recovery needs.

A true business continuity solution will protect your data across on-premises and cloud-based IT environments.

Sources: [1]Beyond Technology, [2]National Archives & Records Administration, [3]Depository Trust & Clearing Corporation, [4]The Ponemon Institute

BinaryLogic Inc.
2020 Scotia Place Tower One
10060 Jasper Avenue, Edmonton, AB T5J 3R8
(780) 665-6677 | info@01logic.ca
www.01logic.ca

BINARYLOGIC