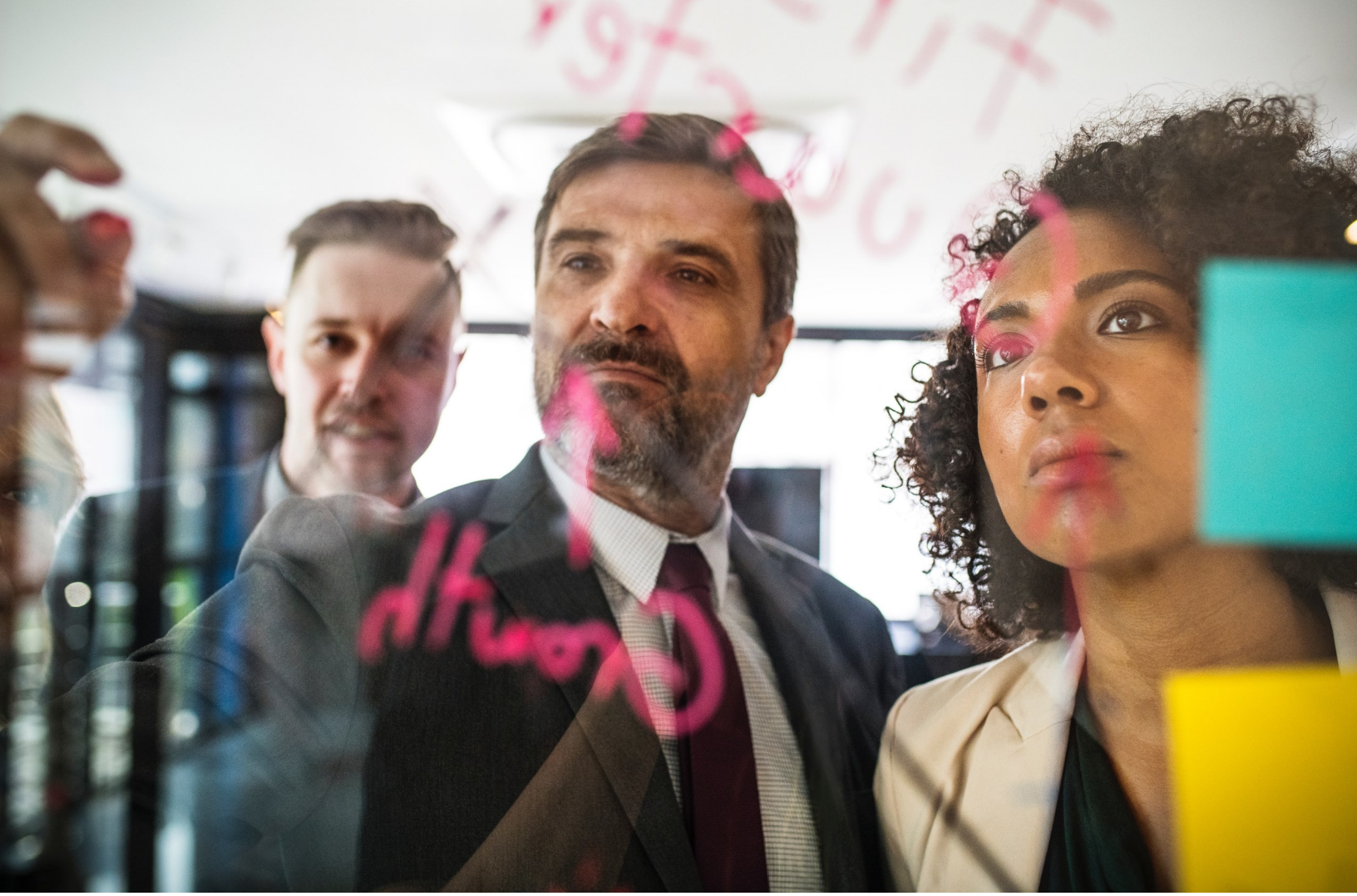
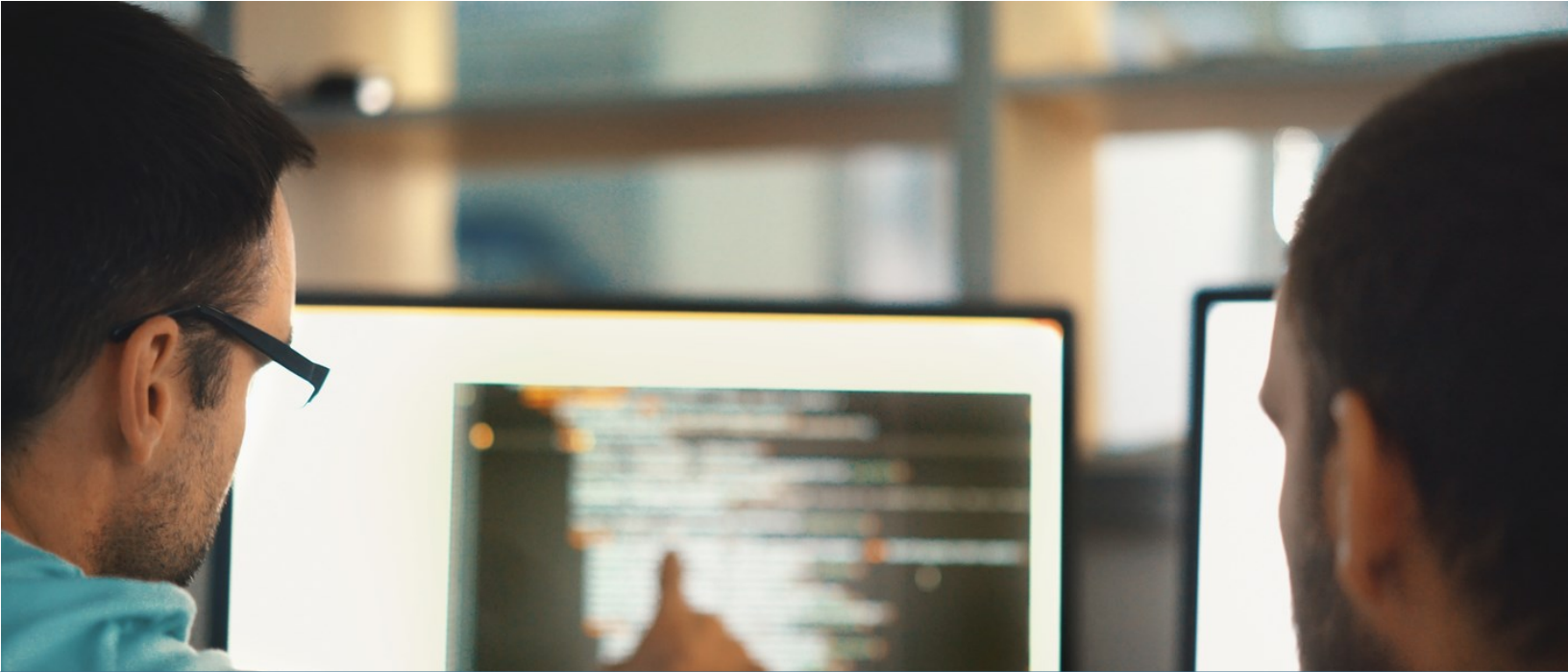


An RIA Firm's Guide to Business Continuity and Disaster Recovery

Is your RIA firm resilient enough to withstand short or long-term interruptions to its operations? This guide breaks down some of the potential costs of business interruptions and why far too many RIA firms don't have a solid business continuity plan in place.

RIA WorkSpace



Business Continuity and Disaster Recovery

Most small and mid-sized RIA firm's aren't doing enough when it comes to business continuity and disaster planning.

As a small or midsized RIA firm, you owe it to yourself, your employees, stakeholders, and clients to honestly answer this one question:

> Is your business resilient enough to withstand short or long-term interruptions to its operations?

The answer should be immediate. If you have to pause or think for a second before responding, the answer is no.

Each day of business brings with it unforeseen risk. Whether it's catastrophic weather conditions, cyber- security threats, or the vulnerabilities of the technology we're dependent on to perform daily work functions, there must be both a business continuity (BC) and disaster recovery (DR) plan in place. There must also be complete confidence in the effectiveness of the BC/DR strategies that are implemented.

Only 50% of businesses have a continuity plan in place to protect their entire business IT infrastructure.

- VMware Inc

The truth of the matter is most small and mid-sized RIA firms aren't doing nearly enough when it comes to continuity and disaster planning. You work in an industry where you store very sensitive data about your clients and the risk of losing this data is so great. Yet according to a report by VMware Inc, only 50% of businesses have a business continuity plans in place to protect their entire business infrastructure.

A few years ago, a study conducted by Forrester Research concluded that 66% of businesses with fewer than one hundred employees admitted to having no tested response to issues like a downed server or network, disasters, emergencies, and power outages.

This e-guide breaks down some of the potential costs of short and long-term business interruptions, why far too many RIA firms don't have a solid business continuity/recovery plan in place, and the necessary steps RIA firms can take to get prepared.

A Competent Disaster Recovery Plan Is a Must

Often misconceived as a problem for the "big guys," business continuity is a concern for RIA firms of all sizes – whether you have 5 or 5,000 employees. The costs of having no solutions in place are too high for many smaller firms to rebound from. Several hours of unplanned downtime can result in thousands of dollars lost each hour.

That's the kind of disruption a small RIA firm may face from a shorter-duration tech issue or power outage. Imagine the consequences of longer lasting outages, where a business may be down for days or weeks, as seen in natural disasters like Hurricane Sandy and Hurricane Katrina, or acts of terror like the 2001 World Trade Center attack.

Beyond the immediate tangible costs of outages like lost productivity and revenues, there is also an intangible domino effect that may be harder to quantify. The repercussions can greatly exacerbate the total losses over time, for instance:

Clients Moving to a Competitor

The web hosting company 1&1 Internet Inc. reported that 72% of web users admit to abandoning a business for a competitor if they can't instantly access a company website or encounter numerous error messages, problems placing an order, or issues accessing online features/support. People want immediate gratification today and will take their dollars elsewhere if they don't get it. Even more alarming is the fact that 58% are likely to never return, which means the loss of long-term revenue streams. Perhaps they may be more forgiving in the event of a crisis like a natural disaster but there will still be those who go to a competitor and never come back.

Word-of-Mouth/Negative Brand Reputation

Thanks to the power of social media, those frustrated by instances of downtime will take to Facebook or Twitter to quickly spread negative messages. Brand building and reputation management are critical to RIA firms. Any negative attention and publicity brought on by downtime can have long lasting consequences.

Downtime can result in lost customers, damage to your brand and reputation, and unhappy employees.

Disgruntled Employees

In small firms, the burden of troubleshooting recurring tech issues or getting a system back online will typically fall upon the shoulders of an already busy, possibly overworked, employee. This multi-tasking employee will have to sacrifice bigger priorities to constantly do damage control. He or she will sometimes have to do this outside of normal work hours and may be pulled away from projects that generate revenue. If they aren't happy about this, they may seek employment elsewhere. Both high turnover and the inability to use an employee's knowledge and skill set for revenue generating tasks are costly to small-to-midsized RIA firms.

RIA Firms Aren't Prioritizing Disaster Recovery Plans

Businesses are fueled by information. They are defined by their ability to efficiently and safely handle the data and vital information they generate or process on a daily basis. It is this data that keeps their day-to-day business functioning, ensuring optimal client service and interaction.

While protecting data is a priority for large enterprises, small-to-midsize business owners have the same responsibility but are challenged by

limited budgets. For a start-up, the entire focus may be client facing, with few resources directed at anything not driving short-term revenues.

This means far too many RIA firms today are failing to employ some very basic safeguards to ensure BC/DR. Most disruptions could be reduced or eliminated altogether by even the most basic BC/DR plan.

Why aren't more RIA firms taking these precautions?

1. They Feel as if They Can't Afford It and They're On Their Own:

Decision makers may know they're living on the edge without a tested strategy, however, they don't realize that new technology trends, and the availability of managed service providers (MSPs), can reduce costs and save on resources. MSPs can leverage their knowledge of an RIA firms specific needs with the numerous cloud and hosted backup and recovery tools currently available today.

Globally, companies lose $700 billion a year because of IT downtime.

2. Failure to Recognize a Problem

Many RIA firms don't think about business continuity or disaster recovery until its too late and they're scrambling to recover after being taken down. It's ironic since so much focus goes into keeping a business sustainable by growing sales, or outdoing the competition, yet a vital part of "staying in business" is overlooked when it comes to their supporting technology.

3. Intimidating and Complex Planning Tools

RIA firms looking to streamline costs and simplify procedures will sometimes write off BC/DR practices as unnecessary. Those who do recognize the importance of preparedness are often overwhelmed by the complex technical jargon that accompanies disaster recovery planning and don't know where to begin when they hear terms like "business impact analysis" and "risk assessments."

Three Steps to Improved Disaster Recovery Planning

Step 1 – Recognize the Need and Importance

Business continuity and disaster recovery strategies tend to be on the to-do lists of many RIA firms, but they are often delayed as more urgent business issues emerge. Enterprises lose $700 billion a year because of IT downtime which includes lost productivity, lost revenue, and the actual cost to fix the problem that lead to the downtime. It's smart business to make business continuity and disaster recovery planning a priority.

To structure a solid disaster recovery plan, RIA firms must be prepared for all possible disruptions. It is important to note that business continuity goes beyond being prepared for natural or man-made disasters. We are now so technologically dependent that BC/DR plans must be in place to counter any disruption – big or small - that threatens business and profitability. Internal technical or infrastructure failures or cyber attacks are obvious examples. Small internal "single-points-of-failure" can bring down an entire operation.

Step 2 – Impact Analysis and Risk Assessment

Constant availability is critical to success. In order to minimize downtime, it's important to determine what technology is behind each phase of your business operations. Knowing the technology infrastructure of your business allows for a comprehensive impact analysis and a better grasp of the impact on business operations when specific technology fails or becomes unavailable - even for a short period of time.

Determining what could unexpectedly bring down each piece of that infrastructure is risk assessment. Risks come in the form of either internal or outside threats.

Internal threats can be anything from an application failure, disk crash, and server malfunction to human error or a bitter employee.

External threats can vary depending on location – natural disasters like hurricanes, earthquakes, tornados, floods, and fires, as well as man-made events like power outages, acts of terror, and accidents can knock out services. Additionally, our dependency on technology leaves RIA firms susceptible to cyber-attacks like malware, computer viruses, phishing schemes, and the theft of personal mobile devices used for work purposes.

While **major disasters** do occur, and shouldn't be overlooked, it is the smaller **everyday disruptions** like power outages, server crashes, email issues, equipment failure, and lost or corrupted data that pose the bigger risk to business. Doomsday prepping may be the rage these days, but a sound BC/DR plan typically begins by focusing on addressing the day-in and day-out disruptions first.

Documenting, reviewing, communicating, and testing the effectiveness of smaller response scenarios will better prepare businesses for potential disasters and longer-term disruptions.

Step 3 – Look to Recent Tech Trends That Simplify Planning

Recent technology developments like server and desktop virtualization, cloud computing, and mobile devices are beneficial to RIA firms looking for BC/DR solutions.

Virtualization

BC/DR preparedness may be the most compelling reason to consider virtualization. Virtualization allows businesses to condense data and applications onto fewer servers - taking up less space and consuming less power. Virtualization allows small-to-midsized RIA firms the benefit of high availability (HA) without the added expense of building a backup data center. Operations can be restored faster as the entire system can be brought back in a single virtual container.

Cloud Computing

More firms are moving to the cloud for backup services. The cloud has enabled small and mids sized RIA firms to backup operations away from their primary location and enhance their business continuity process at a reduced cost.

Cloud-based Software-as-a-Service (SaaS) packages often come with built in business continuity solutions that can automate data backup processes onsite or off-site – spreading out risks and minimizing the impact of a disaster. Data, servers, software, and tools can be stored in the cloud and remain safe if a business is hit by a computer virus or disaster.

The cloud also allows remote workers to access an organization's communication and collaboration tools, further allowing for "business as usual" in the event of a serious disruption.

Conclusion

Although it is understandable that ownership and upper management at small to midsized RIA firms are hesitant to spend money, BC/DR planning is a lot like insurance. It's human nature to think that bad things won't happen to you, but the investment pays off when you're hit by an extreme event or emergency.

New technology trends and the backup as- a-service, remote backup, and online backup services provided by MSPs have given RIA firms the ability to safeguard their business operations at a reasonable cost. Money and resources can no longer be an excuse for a lack of solid BC/DR solutions. There is way too much at risk.