



WWW.NEVERFAILGROUP.COM

PREDICT · PROTECT · PERFORM

Continuous Availability

High Availability
Disaster Recovery
Data Protection



Continuous Availability

Protecting Your Legal Business through IT Outages and Disasters

PROTECTING YOUR LEGAL BUSINESS..... 3

BUSINESS INTERRUPTION 3

INFORMATION AVAILABILITY..... 3

HOW IT OUTAGES AFFECT YOUR BUSINESS..... 3

INFORMATION LOSS 4

PRODUCTIVITY..... 4

CLIENT AND CORPORATE RISK..... 4

REGULATORY COMPLIANCE..... 4

ALIGNING THEORY AND PRACTICE..... 4

MODERN BUSINESS, MODERN SOLUTIONS 5

FINAL THOUGHTS 6

ABOUT NEVERFAIL..... 6

NEVERFAIL LEGAL CUSTOMERS..... 6

PROTECTING YOUR LEGAL BUSINESS

Business Interruption

On average, law firms have the highest percentage of revenue-generating workers of any major industry in the world. The reliance on IT within the legal industry, from attorney communication to back-office processing, is immense. Despite this, the majority of law firms lack effective plans and solutions to deal with interruptions to the IT service. Business continuity, disaster recovery and old-fashioned hardware failures have the potential to bring firms to their knees.

The impact of natural disasters, malicious attacks, rolling blackouts and power outages has raised the importance of disaster recovery strategies. But what about the more mundane causes of data loss and IT outages? Hardware failures happen, configuration mistakes occur, and even seemingly unrelated problems like an air-conditioning failure can cause computers to go down.

When failure occurs, what is the impact? At best, it may be a small interruption in service, but at worst a full data recovery must take place. How much business downtime can your business tolerate? How much data loss is acceptable, and at what cost?

This paper explores some of the implications of current approaches to data protection, disaster recovery and high availability of business critical systems. It also discusses adopting more appropriate strategies and technologies to significantly reduce business risk and increase productivity and business performance.

“One of the limitations of relying solely on tapes is the possibility of corruption, of not getting all the information from the tape. Timeliness also is a factor. Even if the tapes are perfect and you get 100 percent off the tapes, you’re still talking about some extended time required to restore the information. This could be days, depending on what sort of information you have.”

**Stone Pigman
Walther Wittmann**

Information Availability

A law firm’s most valuable asset is information. From briefing notes to client correspondence, document management systems to email, everything used to efficiently run a business depends on IT managing information. There are multiple threats to the IT systems, and all can result in data loss and/or downtime.

To protect against data loss, a backup is typically run every 24 hours. Firms may be shipping backup tapes off-site to protect against disasters. This is all good practice, but what are the implications of relying on such a strategy?

How confident are you that your backup/recovery regime is protecting you from information loss?

IT downtime may not be a result of data loss. It may be as a result of planned hardware maintenance, hardware failure, or external factors such as planned power shutdowns. In rare cases,

there may be a general disaster. All interruptions need to be planned for.

How IT Outages Affect Your Business

The risks associated with losing a critical IT system are very significant. It is critical that firms look at the wider impact that loss of email, a database, or a document server will have on the business.

INFORMATION LOSS

Assuming there is a daily backup at midnight, and the following day work starts at 8am, a disk failure means eight hours of work has been lost. By utilizing the backup tapes, most data can be recovered, but critical documents will be lost and significant business disruption will be unavoidable.

Of course, losing eight hours of data will be painful, but for some companies the consequences will be much worse. It's a well known fact that backup tapes frequently are not complete. Today's backup may not have been run for perfectly good reasons. There may be a media failure meaning the tape could not be read. Either way the data loss is not eight hours, it's sixteen hours (assuming an eight hour day and that the previous day's backups were successful).

If the failure affects business critical systems such as email, matter management or document management the impact may be greater. Documentary records of critical decision paths may be lost, along with evidence.

PRODUCTIVITY

Your fee-earning employees are the key to success or failure, with billing increments at fifteen minutes or even less.

While IT is recovering data from backup tapes, critical systems are not available. Information is not available; advice cannot be given and decisions cannot be made. In the meantime, you are losing money.

How much time will be spent recalling email conversations, retrieving case notes, re-communicating with clients and suppliers to replace the lost data?

Even if your firm has moved to a continuous data protection strategy to minimize data loss, a recovery will still be required resulting in system downtime.

CLIENT AND CORPORATE RISK

In today's fast moving and competitive world, timely access to information makes the difference

between success and failure. From ancient armies to modern law firms, keeping lines of communication open has been critically important.

The adoption of mobile devices, such as RIM's BlackBerry, bears witness to how the immediacy of information is the foundation of the business. The ability to receive compelling new evidence during a trial can directly affect a verdict. Having at hand the latest economic and regulatory indicators during a corporate acquisition negotiation can directly affect shareholder value.

The role of mobile information is well established in modern law firms. When the email infrastructure or the BlackBerry Enterprise Server goes down and the information flow disappears, what is the impact on your firm?

REGULATORY COMPLIANCE

As always, the regulatory landscape influences the way in which data protection and business continuity should be viewed.

Sarbanes-Oxley, The American Bar Association, The UK Law Society and governing bodies all around the world comment on the need for a solid business continuity plan. Business continuity plans that embrace disaster recovery and extend to protecting information systems are not nice to have- they are essential.

There are clear requirements around data and document retention. What happens in years to come if there is a "hole" in the information trail as a result of a data loss? How will this affect your ability to demonstrate adherence to best practice? What exposure will you have?

Aligning Theory and Practice

There are a variety of approaches in each industry to business continuity and disaster recovery. What seems to be common across all industries, though, is the discrepancy between theory and practice.

A large number of organizations have business continuity and disaster recovery plans in place.

A much smaller proportion has actually tested those plans, particularly from an IT perspective. Even when relying on pure backup recovery-based solutions, it is vital to test the effectiveness. When did you last carry out a recovery from a backup tape? Only by doing this on a regular basis can you have a good level of confidence that your information is protected.

Carry out test recoveries on servers in your data room and at your off-site disaster recovery facility, but don't just test the ability to recover the data. Test that the data is compatible with your application backups in order to prevent a team-consuming rebuild of the entire email software infrastructure..

Modern Business, Modern Solutions

Today's law firms should not be relying on outdated backup/recovery software. It should certainly not have disaster recovery plans that are untested, and are not underpinned by effective technology.

There are some basic principles of disaster recovery that can greatly reduce the risk to your company whether an outage comes from an external disaster, or planned IT maintenance.

Your overall goal should be to maintain continuous, uninterrupted availability of the most critical applications. These will include email, BlackBerry (if appropriate), databases, content management systems and web sites.

Make sure you have a reliable, stable platform before implementing a disaster recovery plan. Outages are often caused by poorly configured systems, insufficient hardware resources, and even unreliable network connections. It's worth doing a health check now.

Take the attitude that recovery from backup is a last resort; after all, "recovery" by definition will disrupt business.

Invest in redundant systems. For example, make sure you maintain a replica copy of critical data and applications on a standby server. Do this by using software which copies data in real-time so you won't lose data in the event a disk failure. Best practices include keeping the copy in a remote site to avoid losing data in the event of an external factor such as a flood. Because you have the data protected online, up to date and in its original form, you won't lose anything.

The next stage is to make sure you have software that supports failover, so that the replica copy becomes the primary data. For this to work, applications such as Exchange, or the BlackBerry® Enterprise Server (BES), must also have been replicated so they are in step with the data. You don't want your systems to be down because a security patch has not been applied, or the anti-virus is not up to date on the standby system.

"Test and validate everything."

Jackson Walker

One of the most common complaints about availability is that email

outages aren't discovered by IT, but rather by an end user. Often a user notices it has been several hours since a message was received on his or her BlackBerry and will have to notify IT. Consider making failover automatic by using software to monitor the state of email, or the BES and be proactive. Make sure the failover doesn't force users to logout or reconnect. There is nothing worse than a partner calling the IT helpdesk complaining that email has stopped flowing, only to discover that the issue was fixed hours ago and simply restarting Outlook would have enabled work to continue.

Finally, don't forget what happens when the crisis has finished. How do you get back to running on the primary system? The disruption has ended or been fixed, necessary hardware has been replaced, but users must still logout for hours while the original applications are rebuilt. Switching back after the disruption should be seamless and without interruption to get a firm back to productivity as soon as possible.

Final Thoughts

There are a multitude of reasons why IT systems fail. There is nothing special about law firms that make them more susceptible to failure, but the impact of failure on your firm may be much greater than other industries.

The collaborative nature of a legal firm and the reliance on immediate access to information means the impact of outages is proportionally greater. Deadlines are missed, consultations don't happen, productivity dies and your reputation is at stake.

If you put in place the right data protection, high availability and disaster recovery solution you can be confident that even if a disaster strikes your IT systems, business continues...

About Neverfail

The Neverfail Group is a leading global software company providing affordable high availability, disaster recovery and data protection solutions for mission critical systems.

Neverfail's software solutions enable users to remain continuously connected to the Microsoft[®] Exchange, Domino[®], BlackBerry[®], SharePoint[®] and other Windows[®] based applications irrespective of hardware, software, operating system, or network failures.

Neverfail's mission of eliminating application downtime for the end user delivers the assurance of business continuity, removes the commercial and IT management costs associated with system downtime and enables the more productive use of IT resources.

Neverfail Legal Customers

Law Firms using Neverfail technology to protect their business, increase productivity and reduce risks associated with IT outages and disasters include:

Aird & Berlis LLP
Bilzin, Sumberg, Baena, Price & Axelrod LLP
Blue Williams
Cozen O'Connor
Grancell, Lebovitz, Stander, Barnes & Reubens
Hartman, Simmons, Spielman & Wood
Lau, Lane, Pieper, Conley & McCreadie
Leydig, Voit & Mayer
Munger, Tolles & Olson LLP
Shutts & Bowen LLP
Stone, Pigman, Walther, Wittmann LLC
Rosenberg & Estis
Jackson Walker LLP

More information can be found at

www.neverfailgroup.com.