Acronis

WHY LAW FIRMS NEED CLOUD DISASTER RECOVERY

Developed for law firm IT personnel and managed service providers supporting law firms

Table of Contents

Introduction

Law firms increasingly rely on technology, and a technology disruption for a few days or even a few hours can result in the loss of billable time, regulatory non-compliance penalties, security breach, or worse. When people think of disasters, they typically think of hurricanes, tornadoes, fire, or floods but for a law firm, even a failed server or network outage can be a disaster.

If your firm has 20 lawyers who bill out at hundreds of dollars per hour, even one hour of network downtime per month means that your firm will lose $54,000 (based on $225/hour billable rate) in billable revenue per year; and that does not even include other costs associated with downtime. If a serious disaster happens and the firm's operations are down for a week, that is $180,000 lost in billable revenue. Protecting your law firm's data and ensuring business continuity is critical to your firm's continued success.

In this document, we will discuss the business continuity and disaster recovery (DR) issues that are critical to the legal industry including:

- The exponential growth of data
- Ethical and key compliance regulations impacting law firms
- Security best practices
- Tips for reducing downtime

The core asset of every law firm is data, and keeping this data secure and available can be a complicated task. However, if you follow the best practices discussed in this document, you can keep your law firm's data secure and highly available and protect your firm from lost revenues, compliance penalties, loss of client trust and customers, and damage to your reputation.

Your firm cannot ignore data protection. Read this document and learn about disaster recovery and the best ways to implement it.

Exponential Data Growth

In preparation for a case, a law firm collects a large amount of data, much of it personal and confidential. According to an IDC study, "By 2020, the digital universe will contain nearly as many digital bits as there are stars in the universe. It is doubling in size every two years and by 2020 the digital universe — the data we create and copy annually — will reach 44 zettabytes, or 44 trillion gigabytes."

Data is growing exponentially at law firms as well. This is attributed to the transition from paper to a digital environment, the availability of new technology, and the rise in use of email attachments and higher-resolution images.

Not only are the volumes of client data growing, but also the concept of Big Data in law firms is starting to take shape. In a recent article written by Joseph Raczynski, Legal Technologist/ Futurist at Thomas Reuters Legal, he states, "Over the course of the next several years, I predict that many law firms will begin hiring data scientists…In fact, the analysis that IBM Watson Analytics puts forth states that most firms estimate that they only analyze 12 percent of their data currently and that 88 percent is left on the dark-grained, bamboo-laden law firm floor."

To meet this rise in data growth, your law firm needs a scalable business continuity and data protection solution that can scale to meet your data retention and data availability needs. Building this solution in-house or purchasing an on-premise solution can be expensive, complex, and time-consuming. On the other hand, employing a scalable cloud solution can save your firm money because you pay only for what you use.

Key Ethical and Compliance Regulations

Law firms must meet various ethical and regulatory compliance requirements:

- Legal ethics that regulate safeguarding client property during emergencies or disasters
- Industry regulatory requirements that govern how you manage and protect the data your firm holds on behalf of its clients
- Compliance requirements that apply to outsourced data centers

Legal Rules of Professional Conduct

The American Bar Association's ("ABA") Model Rule of Professional Conduct

An August 2015 article, published in Emergency Management Law by William Gribble, MPA, CLEP, talks to the responsibility a U.S. lawyer has with regards to safekeeping a client's property including case files and documents. The following are excerpts from this article.

As noted, *"The American Bar Association's ("ABA") Model Rule of Professional Conduct ("Model Rules") 1.15 requires a lawyer to safeguard client funds and other property entrusted to the lawyer during representation of the client. More specifically, Comment 1 to Model Rule 1.15 states 'a lawyer should hold property of others with the care required of a professional fiduciary.'"*

Unfortunately, the Restatement or Model Rule's approach focuses mostly on safeguarding funds and less on other property. However some ethics opinions such as *"Florida Bar's 72-37 provide some insight in expecting a lawyer to 'act prudently' while safeguarding client property."*

So what should a law firm do to meet its ethical obligation? Among other recommendations, Gribble suggests that the firm *"consider storing client property off site with a reputable fiduciary organization that focuses on safeguarding client property either online or in a secure storage facility."*

In concluding, Gribble states, *"It is very safe to assume that rules of professional conduct in the legal profession will not be suspended regardless of the circumstances a disaster may impose upon a community. However, taking the time to develop an emergency action plan will reduce a lawyer's risk of violating ethical standards while safeguarding client property and confidentiality during an emergency or disaster."*

The SRA Code of Conduct 2011

U.K. law firms are governed by the "hazy directives" of Principal 8 of the SRA Code of Conduct 2011. This Principal states that you must "run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles." Furthermore, the outcomes in Chapter 7 states:

7.1 You have a clear and effective governance structure and reporting lines.

7.2 You have effective systems and controls in place to achieve and comply with all the Principles, rules and outcomes and other requirements of the Handbook, where applicable.

7.3 You identify, monitor and manage risks to compliance with all the Principles, rules and outcomes and other requirements of the Handbook, if applicable to you, and take steps to address issues identified.

While the SRA Code does not specifically call out the need for a disaster recovery solution, it is difficult to imagine how a firm can adhere to the Principal and Outcomes without a DR solution.

Industry Regulations

Federal and state retention laws regulate data retention policies and law firms that hold data on behalf of its clients are required to abide by relevant regulations. If federal and state laws conflict, you should follow the more stringent policy; it is best to err on the side of caution. Manage your client's data assuming that it can be subject to a claim of a lawsuit. The repercussions of data loss or a data breach can be severe, resulting in costly penalties, ruining a law firm's reputation, and driving away clients

HIPAA (U.S.) – If your organization maintains electronic patient records on behalf of your clients, the Health Information Portability & Accountability Act (HIPAA) requires that your firm have controls in place to manage data integrity, authentication, security, contingency planning, and access and audit controls. Disaster recovery is an important element in meeting these requirements.

Data Protection Act 1998 (UK) – The Data Protection Act governs the protection of personal data on identifiable living people in the UK. One of the data protection principles dictates organizations must take measures to ensure no accidental loss or destruction of, or damage to, personal data. If your firm maintains personal data on behalf of a client, you are subject to the Data Protection Act.

SOX (U.S.) – The Sarbanes-Oxley Act of 2002 (SOX) is legislation enacted by the Securities and Exchange Commission (SEC) in response to high profile financial scandals such as Enron and WorldCom. SOX defines the scope and the duration of the records storage. Not only does it affect your firm's finance department, but it affects your IT department. SOX states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." Failure to comply with SOX can lead to steep fines and possible imprisonment.

GLBA (U.S.) - Under the Gramm-Leach Bliley Act of 1999 (GLB), financial institutions (including law firms) must disclose their information-sharing policies and give clients the opportunity to limit certain types of information sharing by opting out. Even a law firm does not share information in the ways limited by GLB, you must also implement security procedures to keep client information secure. These procedures include:

- Access controls on customer information systems
- Access restrictions on data centers
- Encryption of electronic customer information
- Procedures to ensure that system modifications do not affect security
- Dual control procedures, segregation of duties and employee background checks
- Monitoring systems to detect attacks and intrusions into customer information systems
- Response program that specify actions to be taken when unauthorized access has occurred
- Protection from physical destruction and damage to customer information

Compliance Requirements for Data Centers

SSAE 16, Soc 1, Type II

North American data centers should be audited and certified with SSAE 16, Soc 1, Type II attestation. SSAE is the standard put forth by the Auditing Standards Board (ASB) and the American Institute of Certified Public Accountants (AICPA). It addresses how a service auditor reports on controls at organizations that provide service to user entities; a service organization's controls are likely relevant to user entities' internal control over financial reporting (ICFR). A Type II Report is technically known as a "Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls," reports on the suitability of the design of the controls, and effectiveness of said controls.

ISO/IEC 27001:2005/27001:2013 and ISO9001:2008

Data centers in the U.K. should be ISO/IEC 27001:2005 or ISO/IEC 27001:2013 and ISO9001:2008 certified. This audit and certification process ensures the availability, integrity, and confidentiality of information and network systems. It also ensures that system and quality objectives are reviewed, updated, and amended regularly to guarantee continued suitability.

Best Practices for Security Compliance

Data security is the most important qualifying factor to consider when making the decision for a business continuity solution. Vendor approaches and commitments to security will vary. Keep in mind that any external services you employ are an extension of your primary data center, and must provide the same, if not stricter, security and reliability.

Physical Data Centers

Data centers must employ biometric scanning protocols and around-the-clock interior and exterior surveillance monitoring. Access must be limited to authorized personnel who have submitted to background security checks. Your remote data center must be at least as secure as your internal LAN environment.

Connectivity

Access to your remote data center must be limited to dedicated private lines (e.g., Multiprotocol Label Switching (MPLS)) or over secure Internet Protocol Security (IPsec) VPN connections.

IPsec is a protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream. It can be used to protect data flows between a pair of hosts (computer users or servers), between a pair of gateways (routers or firewalls), or between a security gateway and a host. Data transmitted over IPsec must be encrypted using industry-standard, strong encryption algorithms. MPLS is a mechanism in high-performance telecom networks that directs and carries data from one network node to the next.

Client Divisions

Shared physical resources, such as data centers, require strict attention and adherence to client separation of data to prevent any comingling of data.

Perimeter Firewalls

Protect your networking environment with perimeter security devices to maintain a safe and secure computing environment that meets industry requirements. The perimeter firewall must be configured so that malware, denial-of-service attacks, client-side exploits, and other vulnerabilities are prevented.

Intrusion Detection

An Intrusion Detection System (IDS) detects network traffic that attempts to destroy the security policy of a networked computer environment in order to deteriorate the integrity, confidentiality, and availability of computer resources. The IDS must detect and alert you of network threats in real time, be able to leverage multiple threat signatures, and automatically block attacks.

The Case for Cloud Disaster Recovery

We have made the case for disaster recovery — the cost of downtime, the negative impact to your firm's revenue and brand, and code of conduct and regulatory requirements. Here are four reasons why your firm should consider cloud DR.

- A cloud DR solution is less expensive than an on-premises solution. You only pay for what you use.
- Subscribing to a cloud DR solution is an operating expense versus purchasing an on-premises solution, which is a capital expenditure. In today's economy, it is easier to get OPEX approved vs CAPEX.
- Your firm's IT infrastructure is getting increasingly complex because of the growing volume of data, the increasing number of devices, and advances in technology. Unfortunately, you can only afford to hire IT generalists who do not have expertise in complex IT disciplines such as disaster recovery. A cloud DR solution leverages tested DR automation, best practices, and white-glove support services, allowing your IT department to focus on primary production tasks.
- With a cloud DR solution, you can obtain guaranteed Service Level Agreements (SLA), ensuring that you will meet recovery time objectives (RTO) and recovery point objectives (RPO) for any server or your entire infrastructure.

Today, the industry's leading cloud disaster recovery solutions provide you with a choice of:

- **Hot**, high availability: Your most critical servers will run in parallel in the cloud, eliminating any downtime in the event of a disaster.
- **Warm** stand-by and failover: When a disaster happens, restart primary production servers in the cloud in less than 15 minutes, or an entire data center in less than 2 hours, and restore the services to your users and clients.
- **Cold** backup and recovery: When needed, restore secondary systems from your backups, ensuring tiered, yet complete recovery of the entire infrastructure.

These choices help you limit and manage downtime, increase productivity, eliminate revenue loss, preserve your reputation, and protect your business — while ensuring you are investing in the most efficient solution without under- or over-protection.

Conclusion

It is paramount for your firm to protect its data and its clients' data to ensure compliance, reduce downtime, and protect revenues and the law firm's reputation.

A good cloud DR solution stores your data offsite in a highly secure, highly available data center with failover and redundancy built in. If your building is destroyed or one of your servers failed, you can recover the lost data in accordance with your firm's RTOs and RPOs.

Law firms also have unique requirements, which is why you should choose a business continuity and disaster recovery vendor that has legal industry experience. To understand and be sure that your data is protected in accordance with the laws in your area or for more information, please contact dr@acronis.com.

Useful Links

Acronis Website

Acronis Disaster Recovery Service

Case Study: Bristows LLC

Case Study: Davis Wright Tremaine LLP

Acronis

About Acronis

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete, and safe backups of all files, applications, and OS across any environment — virtual, physical, cloud, and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products were named best product of the year by Network Computing, TechTarget, and IT Professional and cover a range of features, including migration, cloning, and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.