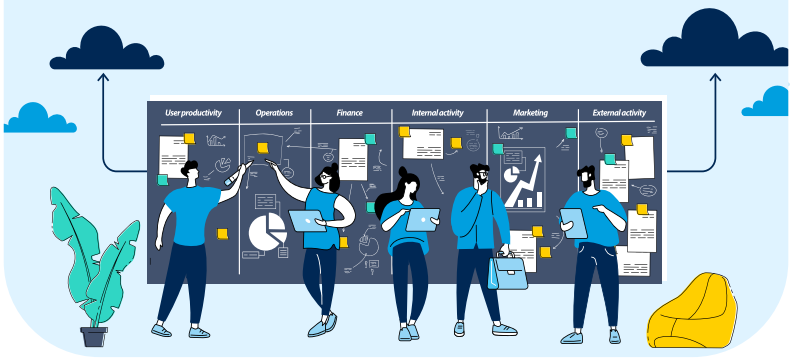
ARTICLE

Dropsuite



A Day in the Life(cycle) — What Data Lifecycle Management Looks Like to Your Clients

As an MSP, your stock in trade is your clients' data. You back it up continuously and protect it for your clients. When disaster strikes, you recover it for them. You ensure that they can always access it.

But how much do you know about data lifecycle management inside each of your clients' businesses? Where does their data come from? Who consumes the data internally? How do they use it? How does it get to you?

When you understand data lifecycle management, you build your clients' confidence in your abilities as their data steward. As a bonus, being conversant in and curious about the ways in which they use data enables you to add value to the managed services you already provide.

This blog post covers the five most common steps you'll see in your clients' data lifecycle management and how it's significant to you as an MSP.

1. How is data created in a business?

How does data originate in a business?

- **User productivity** — Outbound email, inbound email, documents, spreadsheets, presentations
- **Operations** — Programming code, inventions, documentation
- **Finance** — Reporting, tax filings, receipts, payments
- **Internal activity** — Logs, audit trails, status messages, helpdesk tickets, employee communications
- **Marketing** — Lead generation, web forms, user-generated content, blogging, video, social network posts
- **External activity** — Customer transactions, orders, fulfillment

When you think about it, every byte your clients generate is potentially valuable data. Then, add all the bytes that have anything to do with your clients ¬— generated by outsiders like customers, vendors, and channel partners — and you begin to grasp data creation.

The "how" is compounded by the "where," because data is created in plenty of places besides their offices, buildings, and manufacturing plants. Cloud computing, remote work and work from home are business trends driving an increase in the volume of data and the diversity of sources.

It's valuable for you as an MSP to understand your clients' perspective of being awash in data. Asking questions about how and where data is created in their organization shows that you're conscientious about protecting all of it.

2. How is data stored in a business?

Once it's the company's data, it needs to be stored somewhere — on a local drive, on a server, in an on-premises data center or in a public/private cloud.

What's more, whether the data resides on premises or in the cloud, it's subject to being lost, stolen, destroyed, or corrupted. And never underestimate the potential for accidental data deletion, a big yet overlooked threat.

These are the most compelling arguments for backing up the data — preferably, somewhere besides where it currently resides. You wouldn't advise your clients to store files and a backup of those files on the same local drive, would you? That isn't good risk mitigation. Neither is backing up all of their Microsoft 365 content and data to Microsoft 365.

Counsel your clients to follow best practices for backing up their data, including using a different cloud service from the

one they depend on for cloud computing. Advise them on the 3-2-1 approach to backup: save three copies of their data in two different media formats, with one remote copy.

3. How is data used or accessed in a business?

How do your clients use their data?

Using data means accessing it. It's not important for you as an MSP to know who in the organization uses which data for which purpose. But it is valuable for you to develop a picture of how often they need to access it.

Your clients' data lifecycle management is tied to the useful lifespan of a particular type of data, which varies greatly:

A spreadsheet to track event attendance is accessed and used repeatedly in the weeks before the summer picnic. After that, it's never accessed again; it just takes up space.

An email from a departing employee may seem banal. But if a legal claim arises later, the message can help in the company's defense — assuming the company has retained it.

A company's articles of incorporation are accessed and approved once, then rarely accessed again. But they are never forgotten, and nobody would suggest deleting them.

Records in a clinical trial database can span years. Researchers must decide between the low likelihood of accessing ancient records again and the hit to storage involved in keeping them.

Marketing generates and collects leads constantly. But the useful lifespan of leads is short: people change jobs, product lines evolve, and budgets disappear.

You can add value as an MSP by highlighting the role of data lifecycle management in the financial costs associated with storing data for a long time. Your clients may not be focused on it.

As remote work and collaboration tools have become prevalent, sharing has become an important dimension of usage and access. Your clients share data with their own business partners on platforms like Google Workspace, Teams, SharePoint, and many more, which are purely in the cloud. The trend means that they need to think about the lifecycle of data they share externally as well as internally.

Finally, having more data to store also means having more data to secure. Digital transformation means more data from more sources, stored in more places in the organization. The result is an ever-expanding attack surface.

> The longer your clients retain sensitive information, the longer it is a target for exfiltration or malware.

Knowing how long your clients need to retain their data is valuable insight for you.

4. How do businesses maintain compliance and continuity?

Compliance and business continuity form the part of the data lifecycle for which most of your clients rely on you as an MSP.

Compliance plays a role in your clients' data lifecycle management because they are accountable for complying with legal authorities and governing bodies. Compliance of industry regulations and privacy laws is not only how your clients demonstrate good stewardship of data; it is also how they avoid hefty fines.

Regulations vary by industry, and some cross all. Consider a few typical compliance requirements for financial services:

- SEC regulations require that all adviser communications be archived, no matter the communication platform or medium. That includes social media posts, text messages, instant messaging, email and messaging apps. The archive needs to be tamper-proof and authoritative.
- The Sarbanes-Oxley Act (SOX) requires all publicly traded companies in the United States to keep their electronic data for up to seven years, depending on the type of data.
- The Federal Rules of Civil Procedure (FRCP) require that companies be prepared to present electronic records in the event of a lawsuit.
- The Financial Industry Regulatory Authority (FINRA) regulates thousands of broker-dealers with hundreds of thousands of brokers. It requires organizations to monitor and archive broker communications.
- The Gramm-Leach-Bliley Act requires financial institutions to protect the security, confidentiality and integrity of non-public customer information through administrative, technical and physical safeguards.

Data Privacy laws are popping up all over the globe, and data protection authorities are intent on ensuring that companies do not regard penalties as a mere cost of doing business. During the month of December 2021 alone, 57 fines were

levied for violations of GDPR, totaling €246,097,193.

Similarly, the California Consumer Privacy Act (CCPA) is designed to strengthen consumer privacy rights. How does it affect the data lifecycle? The act intersects with your clients' data archiving and backup because subject companies must provide a procedure for retrieving and deleting personal data if the consumer requests it. That means your clients must be able to identify their California customers and find any personally identifiable information (PII) about them.

As for business continuity, the main tools are disaster recovery and incident response (DR/IR). It's how you answer an important question for your clients: What happens to their data when they face a disaster or a data breach and are trying to recover from it? They don't want to be stymied for lack of a serviceable backup, and that's what they turn to you for.

Put yourself in the place of one of your clients that has been breached. While they're dealing with the breach, how do they keep data moving so operations can continue? Can they restore the last backup? If they're doing backup right — in other words, if you as MSP are doing backup right — they'll always have their data in some cadence that keeps their business going. The goal of business continuity is to not lose data at any time, be it to a breach, an outage or a natural disaster.

5. How is data destroyed in a business?

Ultimately, the path of data lifecycle management leads to destruction or deletion.

Every company figures out eventually that there is a cost associated with trying to retain all data forever. In fact, there are a lot of costs associated with that, including physical storage requirements, cloud subscription fees and the risk of keeping sensitive data around for years.

The length of time that your clients are required to retain data and keep it somehow accessible is directly related to compliance. Deciding whether and when to delete data depends on the likelihood that they will need to access and use it five days, five weeks, five months or five years after its creation.

Useful lifespan is a function of the industry, or of a function within an industry. For example, most people in accounting and finance think in terms of retaining data for seven years and of ensuring that specific data can be found in case of audit. Thus, good archiving practices include searchability and customized retention periods.

MSPs can help their clients at this point in the data lifecycle by asking strategic questions. If it's time to destroy a given file or data set, in how many different places does it now reside? Is it on local drives, on a server and in the cloud? How can they be sure to delete all occurrences of it? How can they be certain that deletion is permanent?

Conclusion

In the same way that auto dealers and mechanics don't need to know where the customer drives the car, you don't need to know what's inside your clients' data. You just need know where it comes from and how they use it. And just as that car needs insurance, so does your clients' data. The value you add in backing up their data is that insurance.

By demonstrating awareness of data lifecycle management, you can convince your clients of your able stewardship of their data.

Discover how Dropsuite's Email Backup and Archiving boosts data protection and compliance by helping businesses and MSPs back up Microsoft 365 in the cloud and Google Workspace. Smart organizations protect their valuable business communications with SaaS email backup and archiving solutions such as those offered by Dropsuite.

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com