Data Privacy Detective Podcast – Episode 70: Backup Copies – Preserving Your Privacy and Business Data

Aug 30, 2021

Categories:

Blogs
Podcast
Technology Blog

Authors:

Joseph J. Dehner

Mike Potter's cat bounced on his keyboard years ago. His hard drive cratered, and he lost his data. But he turned this disaster from feline treachery into a career and a company. Backing up data is an essential part of data privacy and retention for businesses as well as for people. Why is this, how does it work, and what's the impact on how we keep and protect our data?

Mike Potter is CEO of Rewind, an Ottawa, Canada based company that backs up, restores, and copies to its cloud critical information businesses store in their SaaS (Software as a Service) applications. Apps sit atop a user's platform. Not unlike cats, they can cause problems. Ransomware attacks, employee mistakes, and many other forces can cause a business to lose essential data even when the platform itself is running well. Having a readily available backup copy can allow a business to continue its customer connections, its bookkeeping, and other essential functions without material disruption. That's the business of Rewind.

Many Rewind customers are retail and other small to midsized businesses that use Shopify, QuickBooks, and other platforms for customer interface and keeping other essential data. While major platforms have good cybersecurity protection, none is immune from a hack attack. But beyond that, a business using a SaaS platform may not realize that its own account remains vulnerable to data loss. When a data loss occurs, the affected business must decide whether this constitutes a data breach, and if so, whether data breach regulations require immediate and usually expensive remedies.

A backup copy can help determine the cause of a data loss, whether from bad actors or accident. It's a starting point to discern what went wrong and how a repeat can be avoided. It may lessen

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

the impact of a ransomware attack if the data held hostage is available to the business anyway without paying a ransom to recoup the data.

When engaging a backup copy provider, a business should consider whether the provider has ample privacy protection for its business. A shaky backup vendor would represent a second vector for hack attacks. A business should vet companies that provide such services. Effective ones will offer services that include keeping data on servers within jurisdictions that have data localization requirements, having funds to afford first-rate cybersecurity protections, offering a 24/7 hotline, and providing excellent customer support.

Tips from Mike Potter to businesses on how to keep essential data private and secure when using SaaS platforms:

- Make sure to use a password manager.
- Use two-factor authentication.
- Vet third-party apps before installing them about their strength and capabilities.
- When you add teammates, make sure they receive the minimum level of permission needed.
- Have a backup available.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons