Why Backups MUST Be Viewed as a Top Security Control

Takeaway from the ILTA/Conversant Group Cybersecurity Survey of Law Firms

In a digital world, organizations of all types live and die by their data. For law firms, this holds especially true: firms are wholly dependent on the information they store and maintain regarding their clients and matters. Should a threat actor access and destroy that data permanently, it would have dire consequences for not only ongoing business, but also reputational trust, a crucial component of law firms' client relationships. Yet only 11% of our responding firms reported backups as a critical security control, and as we will explore, many of the methodologies used to establish immutable, resilient, and redundant backups are lacking across firms of all sizes.

What Is Immutability?

Let's be clear by what we mean by "immutable" (to avoid invoking a definitional problem). This means that data in storage is incapable of being changed, encrypted, or deleted. The only way it should be modifiable is by a two-key simultaneous lock turn (like a nuclear bomb launch we may see in movies) and the expiration of a designated retention period (such as a timed lock on a safe). This is essential for law firms, which are often victimized by ransomware actors who target backups in 98% of attacks (68% of times successfully). Immutable backups are a requirement of many cyber insurance carriers and are the single most important security control of the enterprise—and they themselves require controls around and within them.

Yet, all immutability is not equal. Should a threat actor break controls around one data repository, it is essential that there be several others (we recommend four), all immutable and preferably of different types and differing manufacturers to hedge bets, adding additional layers of insurance against total loss.

How Secure Are Law Firm Backups?

From our study, we see that 38% of respondents reveal that their backup copies are either not immutable or they are unsure whether they are, and only 24% report having multiple immutable copies of all data. While these are concerning statistics, we must dig even deeper to understand whether those reporting one or more copies are immutable are correct. Storage snapshots emerge as the most common form of backup (at nearly double most other backup methods). While this may not be the only method of backup for some firms, it is the most often used, and it cannot be relied upon to be immutable. Only Pure snapshots offer immutability to our standards, and we can see from the ILTA Technology Survey that only 9% of law firms surveyed are using Pure for their shared storage (and all of those are likely taking immutable snaps of all data). Coupling this with the fact that a significant population is using non-immutable local and remote storage, it is

likely that few have the recommended redundancy in immutability to safeguard the firm in the event of determined, targeted backup attacks. Finally, we must shed light on an additional Achilles' Heel in our firms' backup resilience strategies: far too many of our firms have components of backup infrastructure as part of the Active Directory domain. No backup servers, proxies, or targets should be domain-joined, as any attacker that can penetrate the network can then access company data in storage.

Putting Backups in the Forefront to Secure Business Operations

In the end, when your data is gone, so, too, is your business. Backups MUST be considered a first line of defense; learning to defend them with resilience, immutability, and recoverability is essential for firms to ensure continuity of operations.

About the Conversant Group/International Legal Technology Association (ILTA) Cybersecurity Survey and Report

In 2022, Conversant Group and ILTA collaborated to conduct the first-ever cybersecurity-focused benchmarking survey for the legal industry. The survey was targeted specifically at understanding cybersecurity controls, tools, practices, and assumptions in law firms. The results were presented in the report, "Security at Issue: State of Cybersecurity in Law Firms," available for download now. This snapshot presents one key takeaway from the report.