The Forgotten Folder: When Over-Retention Fuels Exposure

By Mardi McNaughton, Peter Ciechanowski, John Sanche & Bruna Kalinoski

In an era where business is conducted almost entirely in digital form, and where cloud storage can be purchased with a single click, it has become easy for organizations to retain far more information than they need to. What once required physical storage rooms and deliberate effort now happens quickly and quietly.

Yet the ease of retention does not reduce its risk. On the contrary, failing to actively review legacy files, identify what must be retained, and destroy what should not be kept, can significantly compound legal, regulatory, and cybersecurity exposure.

Over-Retention: A Risk Multiplier

Cyber incidents are often framed narrowly: if we are breached, how quickly can systems be restored, and what will it cost to regain access to our data? These questions are important, but they overlook a critical issue: what if the compromised data should never have been retained in the first place?

Where a breach exposes information that an organization had no ongoing legal or operational need to keep, the consequences can escalate quickly: regulatory scrutiny intensifies, notification obligations expand, and reputational damage deepens. As recent cases demonstrate, regulatory exposure can arise *even without a cyber breach*.

Cautionary Tales

The Toronto Zoo: Retention Failures Amplifying a Cyber Breach

In a **2024 ransomware attack on the Toronto Zoo**, approximately eighty servers were encrypted and roughly 1.2 million records, including personal information of current and former employees, volunteers, donors, members, and guests, were exfiltrated and posted online.

Through its investigation, the Information and Privacy Commissioner of Ontario (the **Commissioner**) found that the Zoo's document retention policy was more than 30 years old, had been designed for paper record management, and no longer reflected the Zoo's modern digital record-keeping practices. To make matters worse, destruction schedules had not been consistently followed. The Commissioner concluded that the impact of the breach was significantly worsened because the Zoo had retained information well beyond its legal and operational requirements, noting that adherence to retention schedules could have substantially reduced the scope of the breach.

This case illustrates a critical point: cybersecurity failures are often compounded by governance failures. Data that has been destroyed cannot be accessed or disclosed in a cyber incident.

Loblaw: Over-Retention Risks Absent a Cyber Incident

The risk of over-retention is not limited to breach scenarios. In a **2026 report**, the Office of the Privacy Commissioner of Canada (the **OPC**) investigated the retention practices of Loblaw Companies Ltd. (**Loblaw**), in relation to its loyalty program. The investigation was started not in response to a cyber incident, but rather following customer complaints.

Customers alleged they were unable to fully delete their loyalty program accounts. The OPC examined whether Loblaw retained personal information only as long as necessary after account deletion. Loblaw argued that while certain data was retained, it had been "anonymized" and therefore no longer constituted personal information.

The OPC disagreed, concluding that the retained data was not effectively anonymized, that there remained a risk of re-identification, and that Loblaw was therefore retaining personal information longer than necessary, in contravention of privacy legislation. Importantly, this finding arose in the absence of any data breach, underscoring that inadequate retention and anonymization practices alone can trigger regulatory enforcement.

The Long Tail of Regulatory Scrutiny

The timelines in these cases are instructive. The Toronto Zoo breach was initially reported in January 2024 and the regulator's findings were issued over a year later, in June 2025. The Loblaw investigation began in May 2024 and the final findings weren't released until March 2026, nearly two years later.

Organizations involved in cyber breaches and/or regulatory investigations, may be subjected to months or years of regulatory oversight, internal reviews, policy overhauls, customer notifications, and reputational risk management. In many cases, the reputational damage may be difficult, if not impossible, to fully repair. Viewed in this light, the cost of proactive, front-end mitigation is modest by comparison.

What Can Be Destroyed and When?

In short, there is no singular answer. Document retention obligations are governed by overlapping statutes, regulations, contractual requirements, and industry-specific rules. While some records must be retained indefinitely and, in limited cases, in original form, many documents are retained far longer than required out of an abundance of caution.

As organizations transition to digital operations, the categories of documents that must be preserved in original paper or wet-ink form are steadily shrinking. The greater challenge lies in the grey areas, where judgment is required to determine whether continued retention serves a legitimate purpose or merely preserves risk.

Practical Risk Mitigation

Undertaking a records review without appropriate expertise can be daunting. Determining what must be retained, what can be destroyed, and what can be digitized requires legal and operational insight.

Legal counsel can assist in establishing defensible retention frameworks and schedules. Document digitization specialists can help convert legacy records in accordance with best practices, ensuring that digital copies remain reliable and enforceable if ever required in litigation or regulatory proceedings.

Above all, organizations should maintain robust, actively managed retention policies, supported by documented processes to ensure destruction and/or digitization occurs on schedule – not years later, and not only after an incident has occurred.

Key Takeaway

Over-retention is a silent risk. Information that outlives its purpose does not merely sit idle – it expands the attack surface, increases regulatory exposure, and magnifies the consequences of incidents. Proactive retention governance is not a compliance exercise; it is a core component of risk management.

If you are unsure where to begin, members of our **Privacy and Data Protection**, or **Cybersecurity** groups would be pleased to assist.