ARTICLE

The Dangers of Forgotten Data

Data is easy to forget. Especially with the increase in legacy-to-digital transformation, it's easy to overlook unused systems or historical backups. All too often, the focus is on transitioning to new, digital technologies without decommissioning the legacy systems they replace.

Over the past few years, several companies have fallen foul of such "forgotten data," facing serious reputational damage and hefty regulator fines. In this article, we will explore the reasons why data is forgotten, how it can impact a company, and steps that can be taken to address the associated risks and dangers.

Why is data forgotten?

Forgotten data means data that is no longer being actively governed through its lifecycle from creation to defensible disposal. When this happens in an organisation, it runs the risk of breaching several regulations including the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other global privacy regulations.

This can happen for numerous reasons, including:

PROJECT SCOPE

New systems are sometimes introduced to address a "burning platform" such as a crumbling infrastructure or software going out of support. The priority is moving to the new technology. Decommissioning of legacy applications is often not included as part of the project scope or de-scoped once the new application is delivered. In other cases, the problem is "kicked down the road" and positioned as a subsequent phase or project that ultimately never happens.

IT'S ALL TOO DIFFICULT

The data on the legacy applications commonly has no clear ownership or context to enable remediation and defensible disposal. Remediating the data manually is often seen as too time-consuming and reliant on individuals who understand the data (who in some cases may have left the company).

Automating remediation through tooling can assist the process to rapidly identify ROT (Redundant, Obsolete and Trash) data and categorise data that needs to be archived for legal or regulatory reasons. However, most projects do not factor in the complexity of addressing legacy data until it's too late. This is another reason the decommissioning of data gets de-scoped and put under the category of "too difficult."

THERE'S NO ARCHIVE

The company has no strategy or infrastructure to support the archiving of data that needs to be retained for regulatory reasons. The data is therefore left on the legacy system as an "archive," but with little or no governance. With personnel changes, over time, the legacy applications are inevitably forgotten.

Moving data from legacy applications to archives brings that data back under control, aligned to the company's policies, so legacy systems may be retired. This saves time and costs in managing the data through reduced storage and discovery costs (for DSARs, litigation, etc.). This approach also reduces the risk of a data breach or running afoul of data privacy laws for over-retention of personal data.

BACKUPS KEPT INDEFINITELY

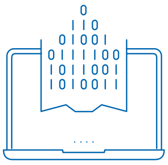
Data can also be forgotten on backups if there are no clear standards on how long they should be retained or how to securely store and handle them. In many cases, processes are also not defined on how to securely destroy or overwrite data held on backups. If there are no standards in place, or controls to check adherence to those standards, then backups can be misplaced, retained indefinitely and completely forgotten.

Backups should be saved for disaster recovery only, and as such are only valuable to support recovery for a designated period. They should not be seen as an archive for the business or legal in the event of litigation.

What are the unforeseen dangers of forgotten data?

Data becomes forgotten because it is often not seen as a priority in terms of effort and budget within a company. But what are the impacts of a seemingly harmless oversight?

LEGACY SYSTEMS EXPOSE YOUR COMPANY TO SECURITY VULNERABILITIES



Data Breach

Data breaches exposed 4.1 billion in the first six months of 2019

Legacy systems by virtue of their age expose your company to data security vulnerabilities. Certain vulnerabilities may not be easy to fix due to ageing technology. Even if there is a fix, the patch is typically delayed (we saw this with Windows XP and WannaCry) because it's more difficult to create a legacy fix – and far lower on the priority list. Legacy systems are often running in companies whilst out of support, exposing the company to cyber and data breach risk.

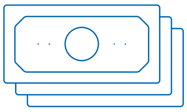
MERGERS AND ACQUISITIONS (M&A) CAN BRING DATA VULNERABILITIES

Regulatory Fine

A large hotelier was fined £18.4 million for failing to keep millions of customers' data secure

If adequate data due diligence (such as ensuring systems have appropriate controls to protect personal data) and remediation are not undertaken as part of an acquisition or merger, the issue can remain like a "trojan horse" undetected and waiting to be exposed by cybercriminals. As an example, a large hotelier estimated that 339 million guest records worldwide were affected following a cyber-attack in 2014 on an acquired company.

LEGACY SYSTEMS ARE COSTLY TO OPERATE AND MAINTAIN



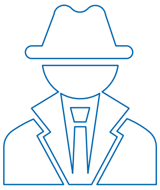
Cost

Legacy systems costs on average 60-80% of IT budgets.

On average, 31% of a company's technology is made up of legacy systems. Maintaining those systems can be a costly burden, with an average of 60-80% of IT budgets allocated to keeping them running.

Decommissioning legacy systems not only reduces the data risks associated with availability and integrity of data but can also release IT budget or be used to justify investment in other projects, such as a remediation project to bring the company's data back under control.

OVER-RETAINED BACKUPS CAN POSE A SECURITY RISK



Accounts Hacked

Backup data from an Online technology platform provider was accessed containing user accounts, passwords, and emails

In 2018, an attacker compromised employee accounts within an online technology platform provider. Exposed data included current email addresses and a database backup from 2007 that contained “old salted and hashed passwords.” This is a prime example of the risks of failing to routinely manage and destroy backups.

ABILITY TO COMPLY WITH DATA SUBJECT REQUESTS

DSR Costs

UK businesses spend £1.59m and 14 years annually on DSRs

Forgotten data is not exempt from data subject requests (DSRs) under GDPR. If data is left ungoverned and undiscoverable in legacy systems, it will be difficult to fully comply with obligations to fulfil an individual’s right to be forgotten and access their data.

Decommissioning legacy systems compliantly and defensibly and remediating data to the new system and/or a company archive not only means the data is more securely managed and governed, but it also means that the data is more discoverable and actionable for DSRs. This reduces the cost and risks associated with not being able to adequately respond in a timely, cost-effective manner to such requests.

Steps to prevent forgotten data

1. Communicate the importance of addressing legacy data risks

   Build a business case to gain executive buy-in to address forgotten data risks. Demonstrate the cost savings that can be made from defensibly disposing and archiving data from legacy systems and the risks that can be avoided in terms of cybercrime, reputational damage and ability to respond more efficiently and cost-effectively to compliance requests.

2. Govern data through its lifecycle

   Effective data governance should encompass the full range of policies, processes and controls that enable data to be governed from creation to disposal, including data management, data privacy, records management and information security. A fundamental data management principle is that data must always be owned throughout its life and appropriate processes put in place to ensure that data does not become orphaned or forgotten. Records management also has a key part to play ensuring a records retention schedule is defined and identifying the rules for defensible disposal or archiving of data. It is then possible to retire and decommission a legacy system and its data according to these rules. Does your company have the appropriate policies, standards and controls in place to ensure that all your data is governed effectively and compliantly?

3. Embed data governance into your SDLC processes

   Embed data governance principles into your System Development Lifecycle (SDLC) and most importantly ensure that end-of-life processes are considered and documented as part of the transition to service. It’s good practice to have an exit plan defined upfront that includes how the system will be decommissioned and the data managed securely and compliantly as part of that process.

4. Implement a standardised approach to application decommissioning

   Make sure you have a standard approach defined and communicated for application decommissioning that includes the remediation of the data they hold. This should include approaches and solutions to archiving data to alternate platforms if the data requires to be retained beyond the active life of the system for legal or regulatory reasons, as defined in the company’s records retention schedule.

5. Prioritise a data hygiene programme to address legacy data risks

   Undertake an audit of legacy systems and dark data such as historic file shares within your company. Ensure that you have up-to-date data privacy impact assessments (DPIAs) for your high-risk systems to understand the level of risk your company holds by retaining the legacy data indefinitely and what steps you can take to mitigate those risks. Record and track the risks within your company’s risk register and based on your company’s risk appetite create a prioritised and costed data hygiene programme to remediate data to address the identified risks.

6. Ensure data privacy is an integral part of your M&A due diligence

   Having a clearly defined set of data privacy roles, responsibilities and processes to support due diligence during M&A activities is critical in ensuring the dangers of forgotten data in the target company do not introduce unforeseen risk and vulnerabilities. Review any acquired systems and data flows and ensure data, privacy and security risks are documented. Develop and define a remediation plan to address these risks and proactively track them through to resolution.

7. Review your data backup policies

To ensure backups don't become forgotten data, have standardised backup processes and schedules including the frequency of backup, the retention period for each backup type, the security of backups and embedded controls to monitor and detect non-compliance. Have detailed processes to recycle (or securely destroy) backup tapes that have expired their retention period. Backup data is only intended for disaster recovery purposes and should not be used as a record archive from which data or records can be retrieved for other purposes by the business. By keeping it beyond its intended purpose you are introducing unnecessary data risk that could come back with a serious bite.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

PETER SHARDLOW
+44 (0) 7929 827812
peter.shardlow@fticonsulting.com

RAJIV RADHAKRISHNAN
+44 (0) 781 428 0318
rajiv.radhakrishnan@fticonsulting.com