## Case Study 1: Cloud Storage and Data Leakage at a Marketing Firm

**Context**

A mid-sized marketing agency allowed employees to use cloud services for collaboration but failed to clearly define or enforce approved platforms. A project team, under tight deadlines, began using a free version of a public file-sharing service not sanctioned by IT.

**Incident**

An employee accidentally shared a folder containing sensitive client data via a public link. The folder was indexed by search engines, leading to the exposure of personally identifiable information (PII) and confidential marketing strategies.

**Outcome**

The company faced reputational damage and a financial penalty under regional privacy laws. A review revealed that over a dozen unapproved cloud applications were in use, bypassing existing controls.

**Key Lesson**

Shadow IT often originates from productivity needs. Lack of guidance and governance around approved tools can quickly lead to data breaches (Huang 2023).

(Gracy 2025)

## Case Study 2: Finance Department Using Unauthorized Budget Software

**Context**

In a large enterprise, a group within the finance department began using a third-party budgeting app without notifying IT, citing frustrations with the speed of internal systems.

**Incident**

The app stored financial data on servers located outside the country, violating the company’s data residency requirements. A third-party audit flagged this non-compliance during routine assessments, which could have triggered legal action from regulators (Mishra 2022).

**Outcome**

The company avoided fines but had to implement costly remediation efforts, including data migration, supplier audits, and updated training. Employees involved claimed they were unaware of the regulatory implications.

**Key Lesson**

Shadow IT may not always be malicious. It often results from gaps between user needs and IT responsiveness. However, even well-intentioned tool use can cause significant compliance risks.

## Case Study 3: Healthcare Provider’s Use of Unauthorized Messaging Apps

**Context**

Healthcare workers at a hospital began using consumer-grade messaging apps (e.g., WhatsApp, Messenger) to share patient updates, citing delays and usability issues in the hospital’s official system.

**Incident**

Screenshots containing patient diagnoses and personal details were shared over these platforms. One phone was later compromised through malware, exposing patient records and violating HIPAA compliance (Webster 2021).

**Outcome**

The breach led to a formal investigation, public criticism, and stricter government oversight. The hospital responded by deploying an encrypted healthcare messaging solution and enforcing stricter mobile device policies.

**Key Lesson**

Convenience often drives shadow IT in high-pressure environments like healthcare. Unapproved communication tools can put patient privacy and institutional compliance at serious risk.

## Case Study 4: Shadow IT in a Software Development Startup

**Context**

Developers at a tech startup adopted various third-party APIs and code repositories (e.g., GitHub, npm modules) without informing security teams. While common in agile environments, many of these libraries had unknown dependencies.

**Incident**

One of the used open-source components had a known vulnerability that was exploited in a targeted attack. The exploit allowed remote code execution on one of the company’s servers (Lee et al. 2022).

**Outcome**

The startup had to take systems offline for forensic analysis. Product timelines were delayed, and the breach harmed investor confidence. Post-incident reviews showed weak version control and no review process for external code.

**Key Lesson**

Shadow IT in technical teams often involves development tools. While innovation is crucial, unvetted components can create backdoors into critical systems.

## Case Study 5: Education Sector’s Unmonitored Online Tools

**Context**

Teachers at a university began using free online quiz and grading platforms to supplement learning, without consulting IT or academic leadership. These platforms required student email logins and stored performance data.

**Incident**

One platform was compromised, exposing student grades and login credentials. Since the tool was not under institutional control, the university had no visibility or recourse during the breach (Gomez 2024).

**Outcome**

The breach prompted an overhaul of digital tool policies in academic settings. A central repository of approved educational tech was introduced, and teachers received training on digital responsibility.

**Key Lesson**

In education, shadow IT often stems from a desire to enhance learning. However, unvetted educational apps can compromise student privacy and institutional trust.

# References

Gracy, S.S. 2025, ‘A global analysis of data breaches from 2004 to 2024’.

Huang, K.B. 2023, ‘Unveiling Shadows: A framework for identifying, assessing, and mitigating risks associated with Shadow IT’.

Mishra, A. 2022, Modern cybersecurity strategies for enterprises: Protect and secure your enterprise networks, digital business assets, and endpoint security with tested and proven methods (English edition), E-book, BPB Publications.

Webster, M. 2021, ‘Do no harm: Protecting connected medical devices, healthcare, and data from hackers and adversarial nation states’, E-book, John Wiley & Sons.

Lee, D.K.C., Lim, J., Phoon, K.F. & Wang, Y. 2022, Applications and trends in fintech II: Cloud computing, compliance, and global fintech trends, vol. 5.

Gomez Orr, S., Bonyadi, C.J., Golaszewski, E., Sherman, A.T., Peterson, P.A.H. & Forno, R. 2024, ‘Shadow IT in higher education: survey and case study for cybersecurity’, *Cryptologia*, vol. 48, no. 1, pp. 26-90.