
# Cyber Secure

# Module 5

# Unintentional Data Sharing

**Author: George Nicholl**

**Student ID: 50095130**

Unintentional data sharing occurs when sensitive information is exposed or accessed without proper authorisation due to human error. Unlike deliberate data leaks or cyberattacks, these incidents are typically accidental - but can be just as damaging. In the age of remote work, collaboration tools, and cloud-based services, the risk of unintentionally exposing sensitive data has increased dramatically.

This module builds on the training video by diving deeper into the common causes, consequences and prevention strategies related to accidental data disclosure.

**What is Unintentional Data Sharing?**

Unintentional data sharing refers to the unintended disclosure of confidential or sensitive information due to carelessness, lack of awareness or misconfigured technology. It can happen during day-to-day tasks such as sending an email, uploading to cloud storage or sharing documents internally.

Unlike external threats, these exposures often originate from within the organisation and are frequently undetected until after the damage has occurred. The impact can include legal penalties, financial loss and reputational damage.

**Common Threats or Mistakes**

**A. Misdirected Emails**

- Emails sent to the wrong recipient due to autocomplete or haste
- 17% of employees admitted to making this error in 2022

**B. Incorrect Attachments**

- Accidentally sending confidential files to the wrong person
- 15% of users acknowledged sending the wrong file externally

**C. Misconfigured Cloud Storage**

- Public access mistakenly enabled on services like Google Drive or Dropbox
- 80% of cloud-related breaches in 2023 involved human error and misconfiguration

**D. Excessive Access Rights**

- Employees ranted more access than necessary, increasing exposure risk
- Weak internal access controls can result in sensitive files being shared unintentionally

**E. Forwarding or Copying Sensitive Data**

- Sharing over insecure channels like personal messaging apps or personal email
- Often done for convenience but creates major vulnerabilities

Together, these behaviours demonstrate how everyday tasks can become security liabilities without proper controls and awareness.

**The impact of Unintentional Data Sharing**

- **Data Breach Costs:**
  The average cost of a data breach reached $4.88 million globally in 2024, with accidental data exposure ranking as one of the top contributors (Varonis, 2024).
- **Regulatory Penalties:**
  Accidental breaches can still violate laws like GDPR or HIPAA, resulting in heavy fines - even when the breach was unintentional.
- **Loss of Customer Trust:**
  Clients expect their data to be protected. Repeated incidents of accidental exposure can significantly damage an organisation's brand and lead to customer churn.
- **Operational Disruption:**
  Data loss incidents can trigger internal investigations, compliance audits, and forced policy overhauls - diverting resources from business operations.

**Real-World Impact of Accidental Sharing**

- Harvard Business Review (2024) – Over 80% of cloud -based breaches were tied to human error
- SC Media (2024) – 95% of all breaches involved a human element, including excessive data access
- ISPartners (2022) – 17% of employees emailed the wrong external contact

These statistics highlight how human error, even when unintentional, is a leading contributor to security failure.

**How to Prevent Unintentional Data Sharing**

**A. Employee Education & Training**

- Conduct regular training on data handling, secure communication and error prevention

- Use case studies and role-specific scenarios for context

**B. Data Loss Prevention (DLP) Tools**

- Automatically detect and block unauthorised sharing of sensitive information
- Integrated with email and collaboration platforms

**C. Access Controls**

- Apply the principle of least privilege to restrict unnecessary access
- Review and update permissions routinely

**D. Email Safeguards**

- Enable delay send, verification prompts, and alerts for external emails
- Prevent accidental delivery of sensitive data

**E. Secure Collaboration Practices**

- Configure sharing settings on cloud platforms with restricted access and expiration
- Use watermarks and file access tracking for accountability

**F. Audit and Monitoring**

- Continuously monitor data movement and conduct audits to detect unusual activity

**Key Takeaway**

Unintentional data sharing is one of the most common – and preventable – cybersecurity risks. By combining practical safeguards, employee training and automated detection tools, organisations can dramatically reduce the likelihood of accidental data exposure.

**Why This Matters for You**

Even well-meaning actions can lead to serious breaches if security isn't top-of-mind. Everyone who handles data plays a role in protecting it. Awareness, caution and secure habits help to ensure sensitive information stays where it belongs.

**Quick Recap: Unintentional Data Sharing Best Practices**

DO:

- ✔ Double-check recipients and attachments before sending emails
- ✔ Use email delay and confirmation features
- ✔ Store and share files securely using access controls
- ✔ Use DLP tools to monitor and prevent accidental leaks
- ✔ Restrict user access to the minimum needed for certain roles

DON'T

- X Don't send work files over personal messaging apps
- X Don't allow default public sharing on cloud folders
- X Don't ignore access reviews or permissions updates

**References**


IS Partners (2022) *Human Error Cybersecurity Statistics*. Available at: https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/ (Accessed: 2 April 2025).

Harvard Business Review (2024) *Why Data Breaches Spiked in 2023*. Available at: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (Accessed: 2 April 2025).

SC Media (2024) *95% of Data Breaches Involve Human Error, Report Reveals*. Available at: https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals (Accessed: 2 April 2025).

Varonis (2024) *82 Must-Know Data Breach Statistics [updated 2024]*. Available at: https://www.varonis.com/blog/data-breach-statistics (Accessed: 2 April 2025).

Varonis (2024) *157 Cybersecurity Statistics and Trends [updated 2024]*. Available at: https://www.varonis.com/blog/cybersecurity-statistics (Accessed: 2 April 2025).