CYBERSECURITY 101 · eBuilder Security

Data Breach

A single attack on one Swedish supplier put personal data on more than 1.5 million people onto the darknet. Here is what counts as a data breach, what one really costs and the change that limits the damage.

WHAT IT IS

A data breach is a security failure that exposes information to people who should not have it. Under GDPR Article 4(12) that covers unauthorised access and disclosure, and also accidental loss, alteration or destruction of personal data. A misdirected email counts. So does a supplier leaking your employee records. Most organisations now meet a breach through a system somebody else runs.

WHY IT MATTERS

12,276

Personal data breach notifications to IMY in 2025, almost 90 percent up on 2024.

IMY annual report, February 2026

1.5 million

People whose data was published after the attack on one Swedish HR system supplier.

Swedish Prosecution Authority, September 2025

58 hours

Between a 10-minute security alert and the compromised device being isolated.

ICO penalty notice, October 2025

WHAT HAPPENED

In January 2025 an attacker reached Sportadmin, a Swedish platform used by sports clubs, through a weakness in its website. Data on more than 2.1 million people was taken and published on the darknet after a ransom was refused. Most of it concerned children. IMY found that the monitoring system raised no alarm during the intrusion, that the alarm came two days later when a server crashed, and that accounts carried more privileges than they needed. Sanction fee: SEK 6 million. (IMY, January 2026)

RED FLAGS TO WATCH FOR

You will not always see a breach from the inside, so watch the signals that arrive from outside too.

- A login from a country or an hour that account never uses.
- Large volumes of data moving to an external destination.
- New accounts or new privileges that nobody requested.
- Logging or security tooling switched off on a server.
- A customer, supplier or researcher telling you your data is for sale.

THE ONE RULE THAT STOPS IT

Shorten the distance between the alarm and the action. Decide today who may isolate a system at 02:00 on a Saturday without asking permission and write that name into the incident plan.

THEN BUILD THE HABIT AROUND IT

- Require multi-factor authentication on every service reachable from the internet, including legacy portals.
- Give every account the least access it needs and review privileges on a fixed schedule.
- Set retention periods for HR records and former employees, then enforce them in supplier systems as well as your own.
- Ask every supplier what they hold about your people and how fast they will tell you if it leaks.
- Rehearse the incident plan once a year with both reporting clocks written into it.

MYTHS AND FACTS

MYTH

Data breaches only happen to big companies.

FACT

IMY took 12,276 notifications in 2025 from organisations of every size. The largest single driver was intrusions at suppliers serving many small customers at once.

MYTH

A data breach means hackers.

FACT

In the incident data the UK regulator publishes, more than three quarters of reported personal data breaches are non-cyber. The most common cause is an email sent to the wrong recipient.

MYTH

If we were attacked, a fine cannot be our fault.

FACT

Regulators assess whether your security matched the risk. IMY set a SEK 6 million sanction fee against Sportadmin after finding known weaknesses left unaddressed.

THE LEGAL DUTY

Under GDPR Article 33 a personal data breach must be reported to IMY within 72 hours of becoming aware of it. If Cybersäkerhetslagen (SFS 2025:1506) applies, in force since 15 January 2026, a significant incident also needs an early warning within 24 hours, an incident report within 72 hours and a final report within one month.

GET HELP

eBuilder Security helps Swedish organisations put detection, response and staff training around the data they hold. Read the full guide at the link below.

Read the Full Article →