CYBERSECURITY 101 · eBuilder Security

Cyber Incident Reporting

When a cyber incident hits, the clock is already running. Here are the deadlines your organisation must meet under NIS2, GDPR, DORA and the main US rules, and the one habit that keeps you on the right side of them.

WHAT IT IS

Cyber incident reporting is the legal duty to tell a regulator, and sometimes affected people, when a security incident crosses a defined threshold. The rules set who you notify, what counts as reportable and how fast. A single incident can trigger several of them at once, and a late or missing report can be an offence in its own right, separate from the breach.

WHY IT MATTERS

52

Cyber incident reporting requirements in effect or proposed across the US federal government alone, 45 of them active across 22 agencies.

DHS, 2023

24 hours

The tightest reporting deadline, the NIS2 early warning and the DORA backstop from the moment you become aware.

NIS2 Article 23; DORA RTS 2025/301

Up to €10M or 2%

The maximum fine under GDPR and NIS2 for essential entities, including for a late or missing notification.

GDPR Article 83(4); NIS2

WHAT HAPPENED

In 2018 criminals used social engineering against staff at 40 hotels to reach the data of about 4,109 Booking.com customers. The company became aware on 13 January 2019 but did not tell the Dutch regulator until 7 February, 22 days late. It was fined €475,000 for the delay alone, not for the breach. (Dutch DPA, 2021)

RED FLAGS TO WATCH FOR

The clock usually starts when you first become aware, so watch for the moments that quietly start it.

- A credible report of a breach from a supplier, customer or partner, even before you have confirmed it.
- An incident that touches personal data, essential services, financial systems or a listed company.
- Pressure to wait for a complete investigation before telling anyone.
- No single person who owns the reporting decision and the deadline.

THE ONE RULE THAT STOPS IT

Start the clock the moment you have a credible signal, and file an initial report within the deadline even before the investigation is complete.

THEN BUILD THE HABIT AROUND IT

- Map which regimes apply to your sector, data and markets before an incident.

- Name an accountable owner for the reporting decision and the clock.
- Prepare a notification template for each authority you may have to tell.
- Rehearse against the tightest clock, a 24-hour deadline, in a tabletop exercise.

MYTHS AND FACTS

MYTH

If we contain the incident quickly, we do not need to report it.

FACT

Reporting turns on thresholds such as risk, materiality or significance, not on whether you fixed it. A resolved incident can still be reportable.

MYTH

The clock starts when our investigation is finished.

FACT

Most regimes start the clock when you become aware. GDPR, NIS2 and DORA all run from awareness, so you file an initial report first and add detail later.

MYTH

A late report is a minor paperwork issue.

FACT

Late notification is a standalone offence. Booking.com was fined €475,000 for reporting a breach 22 days late, separate from any security failing.

THE LEGAL DUTY

In Sweden, NIS2 took effect as Cybersäkerhetslagen on 15 January 2026, with boards personally accountable under Article 20. GDPR, DORA and the main US rules add their own reporting duties and clocks on top.

GET HELP

eBuilder Security helps Swedish organisations map their reporting duties and build an incident response that meets every clock. Read the full guide at the link below.

Read the Full Article →