

Incident Response

Every organisation will face a security incident. Whether it becomes a bad week or a disaster depends on what you prepared before the alert fired.

WHAT IT IS

Incident response is the planned process a team uses to detect a cyberattack, contain it, remove the attacker and recover, then learn from what happened. It turns a chaotic emergency into clear steps and roles, so decisions take minutes rather than hours. The faster and better prepared the response, the smaller the damage and cost.

WHY IT MATTERS

2.66 million dollars

Average saved per breach by having a tested incident response plan, the largest single cost reducer.

IBM, 2025

241 days

Average time to identify and contain a breach, 181 days to find it and 60 to contain it.

IBM, 2025

24 hours

Deadline to send an early warning to MCF under Cybersäkerhetslagen and NIS2.

Cybersäkerhetslagen, 2026

WHAT HAPPENED

In March 2019 the aluminium producer Norsk Hydro was hit by LockerGoga ransomware that encrypted around 22,000 computers across 40 countries. It refused to pay, rebuilt from backups, ran plants manually and shared daily updates. The response cost about 75 million dollars but kept the company running and is still cited as a model (Norsk Hydro, 2019).

RED FLAGS TO WATCH FOR

Signs you may be in the middle of an incident:

- Files suddenly encrypted or renamed, or a ransom note on screen
- Colleagues locked out of systems or accounts at the same time
- A supplier telling you they have been breached
- Unusual logins, data transfers or admin changes out of hours
- Security tools disabled or alerts you cannot explain

THE ONE RULE THAT STOPS IT

Rehearse your incident response plan before you need it. A plan you have run as a tabletop exercise is the one that works at 02:00.

THEN BUILD THE HABIT AROUND IT

- Keep offline, tested backups you can actually restore

- Collect and monitor logs centrally so you spot intrusions early
- Know your critical suppliers and plan for one being breached
- Pre-agree your forensic responders and legal contacts

MYTHS AND FACTS

MYTH

We have backups, so we are covered.

FACT

Backups only help if they are isolated and tested. Attackers target them first, and many teams find out too late that a restore fails.

MYTH

Paying the ransom is the fastest way back.

FACT

Payment is slow, funds more attacks and guarantees nothing. In 2025, 63 percent of victims refused to pay (IBM).

MYTH

We would know straight away if we were breached.

FACT

The average breach takes 181 days just to detect (IBM, 2025). Attackers move quietly to avoid tripping alarms.

THE LEGAL DUTY

Under Sweden's Cybersäkerhetslagen and NIS2, covered organisations must send an early warning to MCF within 24 hours and a full notification within 72. If personal data is exposed, GDPR Article 33 adds a separate 72-hour notice to IMY.

GET HELP

Build your incident response capability before the next alert. Talk to eBuilder Security about managed detection and response.

[Read the Full Article →](#)