CYBERSECURITY 101 · eBuilder Security

Cyber Risk Management

The threats you have found but never fixed are the ones that hurt. Cyber risk management is how you find, rank and close them before an attacker does.

WHAT IT IS

Cyber risk management is the ongoing discipline of finding the cyber threats to your organisation, judging how likely and how damaging each is and reducing each to a level the business will accept. Under NIS2 and Cybersäkerhetslagen it is now a board responsibility, not just an IT task.

WHY IT MATTERS

4.99 million dollars

Global average cost of a data breach in 2026, a record high.

IBM Cost of a Data Breach Report 2026

247 days

Mean time to identify and contain a breach.

IBM Cost of a Data Breach Report 2026

2.2 million

People whose data was exposed through one Swedish supplier breach.

IMY, 2026

WHAT HAPPENED

In August 2025 attackers reached Miljödata, whose HR software serves around 80% of Sweden's municipalities, through an outdated firewall component with known weaknesses. The breach spread to more than 200 municipalities and regions and exposed data on 2.2 million people. In 2026 the regulator IMY fined the company for inadequate security under GDPR Article 32. (Source: IMY, 2026.)

RED FLAGS TO WATCH FOR

Most breaches trace back to a risk that was already known, so watch for the warning signs of risk left unmanaged.

- No single person is accountable for cyber risk at board level.
- You have a list of known vulnerabilities but no plan to close them.
- External logins still work with just a username and password.
- You do not know which suppliers hold your data.
- Your last risk assessment was a one-off, months or years ago.

> THE ONE RULE THAT STOPS IT
>
> **Keep one live risk register that ranks every significant cyber risk, names an owner for each and is reviewed on a schedule.**

THEN BUILD THE HABIT AROUND IT

- Pick a framework such as the NIST CSF or ISO 27001 and work to it.

- Put multi-factor authentication on every external system.
- Patch known critical vulnerabilities fast and confirm the fix.
- Assess supplier risk and avoid depending on a single vendor.
- Test your backups and rehearse your incident response.

MYTHS AND FACTS

MYTH

Cyber risk management is just an IT problem.

FACT

NIS2 and Cybersäkerhetslagen make the board personally accountable for it.

MYTH

We are too small to be a target.

FACT

Attackers hit the weakest link, and supply chains pull smaller firms in.

MYTH

A one-off risk assessment is enough.

FACT

Assets, threats and rules change, so the work has to be continuous.

THE LEGAL DUTY

NIS2 and Sweden's Cybersäkerhetslagen, in force since 15 January 2026, require documented risk-management measures and make the board accountable, with fines up to 10 million euros or 2% of global turnover. GDPR and DORA add their own duties.

GET HELP

Talk to eBuilder Security about running cyber risk management as a managed programme, mapped to NIS2 and Cybersäkerhetslagen.

Read the Full Article →