CYBERSECURITY 101 · eBuilder Security

Security Culture

Most breaches start with a person, not a clever exploit. Security culture is how your people handle risk when no one is watching, and it is now the difference between a near miss and a headline.

WHAT IT IS

Security culture is the shared attitudes, habits and norms that shape how everyone in your organisation handles security every day. It decides whether staff report a suspicious email, verify an unusual payment or quietly work around a control. Technology sets the rules, and culture decides whether people follow them.

WHY IT MATTERS

About 62%

Of breaches in 2026 involved a human element such as error or social engineering.

Verizon DBIR, 2026

40% higher

Success rate of phone and text social engineering compared with email phishing.

Verizon DBIR, 2026

~200 of 290

Swedish municipalities hit by one supplier ransomware attack in August 2025.

Swedish authorities, 2025

WHAT HAPPENED

In September 2023 attackers reached MGM Resorts through a phone call to its IT help desk. Posing as an employee they had researched, they asked for access to be reset. MGM told the US securities regulator the disruption cost around 100 million dollars in a quarter. The systems held. The process for proving who was on the phone did not. (MGM SEC filing, 2023)

RED FLAGS TO WATCH FOR

A weak security culture is visible in everyday behaviour. Watch for these.

- Passwords shared over chat to save time.
- Staff who report a mistake get blamed, so the next person stays quiet.
- Approvals and access granted under pressure without verification.
- Unapproved apps and AI tools used out of sight of IT.
- Security reviews skipped to hit deadlines, with leadership's blessing.

THE ONE RULE THAT STOPS IT

Make reporting a suspicious message or an honest mistake easy, fast and blame-free, so problems reach your security team while there is still time to act.

THEN BUILD THE HABIT AROUND IT

- Give everyone a one-click way to report and thank them for using it.

- Verify payment and access requests on a second known channel.
- Train little and often, with scenarios each team will actually face.
- Have leaders follow the same rules they set.

MYTHS AND FACTS

MYTH

Security is the IT department's job.

FACT

Around 62% of breaches involve a human element across the whole business, so finance, HR and frontline staff are part of the defence.

MYTH

A strong culture means punishing people who click.

FACT

Punishment makes people hide mistakes. Blame-free reporting surfaces incidents faster, which is what limits the damage.

MYTH

You cannot measure something as soft as culture.

FACT

Reporting rates, phishing-simulation results, time to report and staff surveys all track it, so you can improve over time.

THE LEGAL DUTY

Security awareness training is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20. GDPR and ISO 27001 also require organisational measures, meaning how people are trained and managed.

GET HELP

eBuilder Security runs Sweden-based security awareness and phishing-simulation training that turns these habits into everyday behaviour. Read the full guide at the link below.

Read the Full Article →