CYBERSECURITY 101 · eBuilder Security

Shadow AI

Your staff are already using AI tools you have not approved, and pasting company data into them. Here is what shadow AI costs, and the one habit that keeps your data out of tools you cannot see.

WHAT IT IS

Shadow AI is the use of AI tools inside your organisation without the knowledge or approval of IT and security. Staff reach for public chatbots to work faster and paste in documents, source code or customer data. The tools are invisible to security, so confidential information and intellectual property flow out of the company with no one watching, and with no way to govern the tool or report an incident.

WHY IT MATTERS

15 million euro

Fine issued to OpenAI by Italy's data-protection regulator over how ChatGPT handled personal data.

Garante, 2024

2 February 2025

Date the EU AI Act's AI-literacy duty under Article 4 began to apply to organisations.

EU AI Act, 2024

10 million euro or 2%

Maximum NIS2 fine for an essential entity, of global annual turnover, whichever is higher.

NIS2, 2022

WHAT HAPPENED

In 2023 Samsung let engineers in one division use ChatGPT. Within weeks the company found that confidential internal data had been pasted into the tool on separate occasions, including semiconductor source code and the notes from an internal meeting. Nothing was stolen by an attacker. Skilled staff had simply put company work into a public tool to get help faster, and in May 2023 Samsung restricted generative AI on its devices. (Bloomberg, 2023)

RED FLAGS TO WATCH FOR

Shadow AI rarely looks like a breach. It looks like people trying to work faster, so watch for these signs.

- Staff pasting documents, code or customer data into public chatbots to save time.
- AI tools adopted team by team with no sign-off from security.
- Free consumer AI accounts used for work on personal phones and laptops.
- AI output dropped into a report, a filing or a customer message with no one checking it.
- No inventory of which AI tools touch company data.

THE ONE RULE THAT STOPS IT

Never paste confidential, personal or business-critical data into an AI tool your organisation has not approved. If you need AI for the task, use the sanctioned tool instead.

THEN BUILD THE HABIT AROUND IT

- Give staff a sanctioned AI tool so there is a safe alternative to the public one.
- Publish a plain acceptable-use policy that says what may and may not go into AI.
- Keep an inventory of approved AI tools and the data each one is allowed to touch.
- Check AI output before it feeds a decision, a filing or a customer message.

MYTHS AND FACTS

MYTH

Shadow AI is just people using ChatGPT, it is not a real security issue.

FACT

It is the uncontrolled flow of company data into tools you cannot see or govern, which is exactly how confidential information and IP leak out.

MYTH

If we ban AI tools, the problem goes away.

FACT

A ban pushes staff to personal phones and accounts where you have no visibility. A sanctioned safe tool works better than a block.

MYTH

Shadow AI is an IT problem for IT to solve.

FACT

Under NIS2 Article 20 the board is accountable for security measures, so AI governance belongs at leadership level and not with IT alone.

THE LEGAL DUTY

Personal data pasted into an unapproved tool can breach GDPR, and an AI system nobody has inventoried cannot be governed under the EU AI Act or reported under NIS2. NIS2 is in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20, and the EU AI Act has required AI literacy since 2 February 2025.

GET HELP

eBuilder Security helps Swedish organisations bring AI use into the open with governance, monitoring and Sweden-based security training. Read the full guide at the link below.

Read the Full Article →