

Five questions before approving cyber and AI spending

A CEO's checklist | Matt Apps | Pangolin Advisors

Put these questions to your CISO, AI lead and CFO together. Ask for evidence before accepting reassurance. Use the answers to change the budget.

1 After this spending, which serious exposure will still be open?

Ask for the business consequence, the owner and how long it will remain. For any unmet legal duty, require the actual requirement and a dated remedy. "Within risk appetite" needs an explanation.

Decision: bring forward work where the remaining exposure is unacceptable; make any decision to retain risk explicit.

2 In the last recovery test, when could customers use the service again?

Ask for the elapsed time, what failed and what was excluded. Were staff access and critical suppliers included? A successful backup restore answers only part of the question.

Decision: fund work that removes the obstacles to resuming an acceptable service. If recovery is unproven, require a test before accepting the claim.

3 Are we buying more ways to find weaknesses we cannot fix?

Ask which dangerous weaknesses are already known, how long they have remained open and what blocks the fix. What would another tool change?

Decision: if remediation is the constraint, redirect money to engineering, safer changes or replacement. Buy more discovery where missing visibility justifies it.

4 If AI savings fund the proposal, which costs will actually disappear?

Ask the CFO to identify the costs, dates and person accountable, after integration, checking and running costs. Scattered hours saved are not automatically removable posts.

Decision: where cash savings are unproven, revise the case. Better output or avoided recruitment may justify investment, but name the benefit you are buying.

5 Which purchase would you remove first, and what would happen?

Ask management to rank proposals and identify duplication, weak results and delivery bottlenecks. Include the effect of withdrawing existing capability and any legal or service dependencies.

Decision: stop or defer the weakest case where the consequence is acceptable. If every item is "essential", require management to explain the order and trade-offs.

Before signing off: record what changes, who owns it, the evidence you expect and the date you will review it.

Discuss your cyber and AI plans

For an independent assessment, contact Matt Apps: matthew@pangolinadvisors.com

Companion to Cybersecurity and AI: A CEO's Briefing. Evidence and regulatory scope are explained in the paper. Research position: 18 October 2026.

Read the full paper: doi.org/10.5281/zenodo.23532101