

Cybersecurity and AI

A CEO's Briefing

Regulatory expectations, investment and the gaps that remain

Matt Apps | Pangolin Advisors | 18 October 2026

Find the answers you need

The paper follows four questions. Select a section below to go straight to it.

[1 What is expected](#) Which rules apply and what do they require

[2 What is happening](#) What peers are buying and what they are achieving

[3 Is it enough](#) Where spending can leave serious risks unresolved

[4 What should change](#) What to fund, defer or stop

Your cyber budget is going up again. Your AI team wants more money. Both say the business cannot afford to fall behind.

You need to know whether they are right. Can the business survive a serious attack? Are you meeting the rules? Will the next investment reduce a risk that matters, or add another system your people struggle to manage?

There are good reasons to invest. But regulators are still finding weaknesses in recovery, access controls and suppliers. Businesses are buying more technology and planning to spend more on AI. The question is whether those purchases address the weaknesses that could hurt your business.

I'd put the next pound where there is an important gap and a credible way to close it. That could mean engineers to fix weaknesses already found, replacing obsolete equipment or proving that the business can recover. Sometimes it will mean better technology. With AI, be clear about the benefit you are buying. Saving staff time can be valuable without reducing payroll. If a wider rollout depends on lower payroll costs, management needs to show which costs will actually disappear.

The following sections set out the rules, the investment evidence and the decisions I would challenge before signing off the budget.

1 What is expected

Start with the passages that apply to your business. More than one may be relevant; skip the rest.

Select the relevant heading below. These are starting points for checking your obligations, not a determination of your company's legal position.

[UK and EU financial services](#) — Resilience, DORA and UK reporting

[Other EU businesses](#) — NIS2 and digital product obligations

[UK board reporting](#) — Provision 29 and guidance for other UK businesses

[AI use](#) — EU AI Act and existing UK duties

If you run a financial services business

For UK firms covered by the operational resilience rules, the requirement is already in force. Since 31 March 2025, they have had to be able to keep important business services within the limits of disruption they have set during severe but plausible events. Management must understand what those services depend on, test for weaknesses and remedy them. The governing body approves the firm's assessment. [1]

The service is what matters. Restoring a payment system after customers have suffered intolerable harm may still leave the firm short of its obligations.

In the EU, the Digital Operational Resilience Act (DORA) has applied to covered financial entities since January 2025. It brings technology risk, incidents, testing and supplier arrangements under a common regime. The management body retains responsibility, including oversight of an appropriate resilience budget. Outsourcing the technology does not outsource that responsibility. [2]

UK firms also have a reporting deadline: 18 March 2027. The new incident rules cover a wider population than the material third-party reporting rules. Check which apply. Material supplier arrangements can be covered even when they are not classified as outsourcing. [7]

If you run another business operating in the EU

Check whether the EU's NIS2 cybersecurity regime applies through the relevant country's law. It covers specified sectors and generally medium and large entities, with exceptions. Its reach includes some manufacturers and managed IT service providers as well as more obviously critical sectors. Covered management bodies must approve and oversee cyber risk measures. Continuity, supplier security and checking whether controls work are part of the requirements. [3]

If you manufacture a covered digital product for the EU market, the Cyber Resilience Act adds product security and vulnerability-handling duties. Manufacturer reporting requirements began in September 2026; the main obligations apply from 11 December 2027. Selling standalone software as a service does not automatically put you in the same category. [6]

Before funding the response, establish which business activity brings your company into scope. A competitor's compliance programme may address different obligations.

If your board reports under the UK Corporate Governance Code

Revised Provision 29 applies to financial years beginning from January 2026. Boards must report on the effectiveness of material controls under the Code's comply-or-explain framework. Relevant cyber controls can be included. [4]

Do not assume the financial statement audit covers this declaration. The FRC says it does not, and auditors are not required to test every material control the board identifies. Establish what supports your statement. Internal audit and existing tests may provide the evidence you need. [11]

For UK businesses outside these regimes, the voluntary Cyber Governance Code is a useful baseline. It asks leaders to understand critical services, allocate resources effectively and obtain evidence of results. It is guidance, not a legal requirement for every company. [10]

If your business uses AI

The first question is what the system does and what your company does with it. Buying an assistant to draft documents creates different obligations from providing an AI system or using one in recruitment. Calling a product an agent does not determine its legal status.

Under the EU AI Act, current duties include supporting staff AI literacy and, where applicable, telling people they are interacting with AI. Following the July 2026 amendment, requirements for high-risk uses listed in the Act, including certain recruitment applications, start on 2 December 2027. Relevant high-risk systems embedded in regulated products follow in August 2028. Management needs to identify which category each use falls into and prepare for the duties that follow. [5, 24]

A later AI Act deadline is not permission to ignore existing law. Data protection obligations still apply. In UK financial services, Consumer Duty and senior management accountability remain relevant to AI use. [9]

Before accepting “the regulator requires this investment”, expect a clear explanation: which requirement, why it applies, where the business falls short and how the proposal fixes it. A requirement to recover a service is not, by itself, a requirement to buy the supplier's preferred platform.

2 What is happening

Many of your peers plan to spend more. Their intentions give you a view of the market, but they cannot settle your budget.

PwC's survey released in October 2026 found that 84% of security and finance leaders expected cyber budgets to increase. Among security leaders, 58% ranked AI among their leading cyber budget priorities. The pressure to commit more money is widespread. [12]

ENISA's EU study puts cyber expenditure at about 9% of IT budgets, with median annual security spending of €1.5 million. The report says organisations are favouring security technology and outsourced services over expanding their own teams. Those spending figures mainly concern 2024. They are context, not a recommended allocation for your company. [13]

Outside help is common. In the UK survey, 70% of medium-sized businesses used an external cybersecurity provider. Only 30% formally reviewed their direct suppliers' cyber risks, and 13% reviewed risks further down the supply chain. These percentages are not matched company by company, so they do not show that firms outsourcing security also neglect supplier reviews. They do give you a reason to examine your own arrangements: who checks the provider, and what happens if it fails? [14]

Some investment is improving recovery

A joint Bank of England, PRA and FCA publication describes firms investing in protected backups and separate recovery facilities. Some are testing how to rebuild clean systems after an attack and keep essential services running while full recovery continues. [18]

That is a more useful comparison than the size of a budget. What can a similar business keep running, and what has it demonstrated? A smaller firm can use that comparison without copying a bank's infrastructure.

AI ambition is ahead of widespread deployment

Gartner reports that 85% of functional leaders planned to increase AI spending, while 22% reported successful scaling across business units or an AI-first approach. Investment intentions are strong; widespread deployment remains uneven. The survey does not establish that the other organisations have failed. [15]

UK government research gives a mixed picture. Among AI users, 34% reported lower production or operating costs; 77% reported no change in revenue since adoption. These are self-reported results from early 2025 fieldwork. They show benefits in some businesses, not what a current tool will earn in yours. [19]

In the September 2026 ONS responses, 6% of AI-using businesses with at least ten employees reported reducing headcount because of AI. This does not measure quality or output. It does make quick payroll savings a poor assumption on which to fund a rollout. [16]

What you can learn from peers

A spending ratio cannot tell you whether your business needs another security platform. Compare businesses with similar services, dependencies and constraints. Ask what they can do that you cannot, whether the difference matters and what it costs to close it.

Cloud offers a useful comparison. The ECB reports cloud expenses rising from around 4% of banks' IT budgets in 2021 to 17% in 2025, alongside unresolved supplier and continuity issues at some banks. Before AI becomes another large recurring cost, examine the running costs, contractual dependence and ability to change suppliers. That is an investment lesson; it does not predict AI's future. [22]

3 Is it enough

A rising budget can leave serious gaps untouched. The findings below give you specific places to check. Whether they apply to your company depends on its own evidence.

You may have backups without a business that can recover

The FCA's 2026 review found progress, but also self-assessments that did not adequately cover dependencies or support recovery claims with sufficiently severe tests. It identifies weaknesses in the firms reviewed, not a failure rate for the sector. [17]

Your data may be intact while staff cannot log in, a supplier is unavailable or orders cannot be processed. Restoring files does not tell you when trading resumes.

If losing a service could seriously harm customers or threaten the business, ask to see what happened when that service was recovered in a realistic test. What worked? How long did it take? What was left out? Fund the gaps that prevent an acceptable service from resuming. Buying a second copy of everything is not automatically the answer.

Your people may need help fixing what your tools already find

The regulators' 13 CBEST attack simulations in 2025 exposed weaknesses in credentials, permissions, configuration, separation between systems and detection. ENISA separately reports that 28% of organisations surveyed took more than three months to patch critical vulnerabilities. The FCA's frontier AI review describes firms finding weaknesses faster than they could fix them. [20, 13, 21]

Finding another thousand weaknesses achieves little if the team cannot deal with the dangerous ones already known. That is a reason to examine the constraint before buying more tools, not proof that the existing tools were a bad purchase.

Establish where the work is stuck. If visibility is poor, better detection may be justified. If weaknesses are known but remain open, the priority may be engineering time, safer ways to make changes or replacing an obsolete system. Judge progress by the serious attack paths closed, not the number of findings processed.

A critical supplier can leave you with no workable alternative

The UK survey measures supplier reviews, not the ability to survive a supplier failure. Your own continuity evidence has to answer that question. [14]

For the CEO, the priority is the supplier whose loss stops an essential service. A certificate may tell you something useful about its security. It will not settle whether you can continue when it is unavailable.

Where the business cannot tolerate that interruption, spend on a workable response: a tested fallback, a credible recovery arrangement or an alternative supplier. Reviewing every supplier to the same depth would consume resources without reflecting the consequences of failure.

Your improvement programme can itself interrupt the business

The ECB reports that IT change caused 38% of major incidents reported by banks in 2025. This is a banking figure, but the investment issue is relevant elsewhere: introducing improvements can create disruption. [22]

Several sensible projects can rely on the same engineers and testing capacity. Funding all of them does not create the capacity to deliver them safely. Before accelerating the programme, establish what can actually be implemented and supported. A slower sequence may protect the business better than several overlapping launches.

Old technology creates a related decision. NCSC guidance describes the extra protections and recovery difficulties associated with obsolete industrial equipment. For a manufacturer, compare the full cost of keeping it against replacement, including production downtime and safety. Cutting the security budget alone may leave the source of the cost untouched. [23]

AI time savings may not pay the bill

Suppose 100 people each save 10% of their time. That is capacity equivalent to ten full-time roles. It does not mean ten posts can be removed. The time may be spread across different duties, while checking, specialist work and peak demand remain. This is an illustration, not a survey finding.

Better output, avoided recruitment and better service can justify AI investment. A proposal funded by lower payroll needs to go further and show how those costs will leave the business. The survey figures do not answer that for an individual employer. [16, 19]

There is a separate risk when AI can act. An assistant drafting a payment instruction is different from an agent approving the payment. The FCA records firms using permission limits, approvals and validation. Those are reported practices, not new rules. [21]

Before granting consequential authority, demonstrate that the limits work when the system makes a mistake or receives misleading instructions. A human reviewer needs enough time, information and

authority to prevent the harm. Where that has not been demonstrated, restrict the action while testing continues. Useful, low-impact assistance can continue without granting wider powers.

The board may be relying on evidence that answers another question

An application security test does not demonstrate recovery of the whole service. A supplier certificate does not demonstrate your fallback. A financial statement audit does not provide an opinion on the board's Provision 29 declaration. [11]

The problem is serious when the board believes a major risk has been examined and the supporting work excludes it. Establish what existing tests and reviews cover before commissioning more. Independent work is worth buying where an important conclusion remains unsupported, not simply because another report is available.

4 What should change

Break the budget into decisions you can make. Some work may need to accelerate while another purchase should wait. I would challenge it in five places.

Fund the shortfalls you cannot reasonably leave open

Give priority to unmet legal duties and failures that threaten essential services. Require a named gap, a proportionate remedy, an owner and a date. For recovery, the result should be a demonstrated ability to resume the service within the required time. "The project is complete" is not sufficient evidence.

Redirect money where delivery is stuck

If installed tools are finding serious weaknesses that remain unfixed, consider people and remediation before more discovery. If old equipment drives repeated security costs, bring operations and finance into the replacement decision. The best use of the cyber budget may depend on a decision outside the CISO's authority.

Expand AI where the business has demonstrated the benefit

Use results from the actual work, including integration, checking, correction and running costs. Distinguish cash savings from capacity and improvements in service. Keep consequential actions within tested limits. An application can deserve expansion without every proposed use of the same technology deserving approval.

Defer work the business cannot yet deliver safely

If expansion relies on unproven savings, unavailable delivery capacity or controls that cannot prevent serious harm, defer it. Specify what would change the decision: a trial, a test showing the controls work when something goes wrong, or completion of another project. Give that work an owner and a date.

Stop paying for capability that adds no useful value

Look for duplicate coverage, persistent underperformance and services with no remaining business purpose. Check dependencies and legal duties before withdrawing them. Retiring a tool is a valid

decision when the evidence supports it; so is retaining an apparently expensive capability that protects an essential service.

For your next budget discussion, ask management to explain the decisions they want you to make: what must be funded, what can wait, what should stop and what risk remains after the spending. Each recommendation needs evidence and an explanation of the consequence if you decline it.

When you approve the budget, be clear about the decision you are making: which legal shortfalls will be closed, which services will be better protected, which AI benefits justify the cost and which risks you are choosing to retain. Set the evidence and date for checking the result. If a proposal cannot explain what changes for the business, it has not earned its place in the budget.

Discuss your cyber and AI plans

If you want an independent assessment of whether your cyber and AI plans address the risks that matter to your business, contact Matt Apps at Pangolin Advisors.

matthew@pangolinadvisors.com

Sources and evidence notes

Position at 18 October 2026. The legal duties depend on the company, its activities and the relevant jurisdiction. The UK Cyber Security and Resilience Bill remains proposed legislation at this date. [8]

Regulatory findings concern the firms examined. Surveys differ in population, size, definitions and fieldwork dates; their percentages are not combined here. ENISA's sample was predominantly large organisations in high-criticality sectors. PwC and Gartner provide international evidence, not UK and EU spending benchmarks. Recommendations and illustrative examples are Pangolin Advisors assessments. More spending does not, by itself, establish either better protection or waste.

[1] FCA. SYSC 15A Operational resilience. Rules and guidance, especially sections 2 and 4 to 7. [Source](#)

[2] European Union. Regulation 2022/2554 DORA. Articles 4 and 5; application from 17 January 2025. [Source](#) [EIOPA overview](#)

[3] European Union. Directive 2022/2555 NIS2. Articles 2, 4 and 20 to 23. National implementation must be checked. [Source](#) [Commission scope guidance](#)

[4] FRC. UK Corporate Governance Code 2024 and cyber reporting clarification. Provision 29 applies to financial years beginning from 1 January 2026; cyber mythbuster dated 23 September 2026. [Source](#)

[5] European Union. Regulation 2026/1744 amending the AI Act. Revised high risk dates and AI literacy provisions; read with Regulation 2024/1689 and applicable transitional provisions. [Source](#) [Commission implementation timeline](#)

[6] European Commission. Cyber Resilience Act summary. Product scope; manufacturer reporting from 11 September 2026 and main obligations from 11 December 2027. [Source](#)

[7] FCA. PS26/2 Operational incident and third party reporting. 18 March 2026. Final rules apply from 18 March 2027; incident and third party populations differ. [Source](#) [FG26/4 paragraphs 2.1–2.2](#)

[8] UK Parliament. Cyber Security and Resilience Bill stages. Bill 4035; proposed legislation at cutoff. [Source](#)

[9] FCA and ICO. AI approach and data protection accountability. FCA approach updated 2 October 2026; data protection duties apply to relevant processing. [Source](#)

[10] UK Government. Cyber Governance Code of Practice. 8 April 2025. Voluntary governance guidance. [Source](#)

[11] FRC. Auditor responsibilities for the Provision 29 statement. 24 June 2026. Financial statement opinion does not cover the declaration; reading other information is not an assurance engagement. [Source](#)

[12] PwC. 2027 Global Digital Trust Insights. Released 1 October 2026. 3,934 business and technology leaders across 71 countries; quoted measures concern different respondent groups. [Source](#)

[13] ENISA. NIS Investments 2025. Survey of 1,080 organisations, May–August 2025; predominantly large entities in high-criticality sectors. Spending refers to 2024. The 28% patching figure is consistent with Figure 14 and ENISA's release. [Report Release](#)

[14] UK Government. Cyber Security Breaches Survey 2025/2026. Medium and large business supplier and outsourcing measures; reported practices, not tested effectiveness. [Source](#)

[15] Gartner. Only 22 percent have successfully scaled AI across business units. 1 September 2026. January to April survey of 1,303 respondents from organisations with at least USD 50m annual revenue. International evidence. [Source](#)

[16] ONS. Business insights and impact on the UK economy. 8 October 2026. September responses; headcount measure concerns AI using businesses with at least ten employees. Official statistics in development. [Source](#)

[17] FCA. Operational resilience insights and observations one year on. 27 March 2026. Supervisory examples establish progress and weaknesses without a population prevalence estimate. [Source](#)

[18] Bank of England PRA and FCA. Effective practices in cyber response and recovery. 20 October 2025. Observed practices primarily from systemic firms and financial market infrastructures, to apply proportionately. [Source](#)

[19] DSIT. AI Adoption Research. Published January 2026. 3,500 interviews in February to May 2025; impact questions among 700 AI users. Self reported. [Source](#)

[20] Bank of England PRA and FCA. 2025 CBEST thematic. Technical findings from 13 assessments conducted in 2025. Not a representative prevalence survey. [Source](#)

[21] FCA. Frontier AI and cyber resilience. 2 September 2026. Firms reported faster discovery, remediation constraints and operational guardrails. No new rules, guidance or expectations. [Source](#)

[22] ECB Banking Supervision. Upgrading banks capacity to deal with digital risks. 24 March 2026. IT change incident share and third party observations relate to banks. [Source](#)

[23] NCSC. OT secure connectivity principle 1. 14 January 2026. Guidance on obsolete equipment, compensating controls and replacement planning. [Source](#)

[24] European Union. AI Act consolidated text at 27 July 2026. Articles 4, 6 and 50 and Annex III. Role, intended purpose, exceptions and applicable transitional provisions determine the duties. [Source](#) [Article 4](#) [Article 50](#)

[UK Corporate Governance Code](#)

[ICO guidance on AI accountability](#)