GRCPRENEUR EVIDENCE REPORT

From a cyber report to a management decision

Prepared for GRCPreneur by Hassan Sharif | Source review: 19 November 2026

Purpose and source distinctions

A recent publication can make a useful discussion more informed without answering the business's question by itself. This GRCPreneur evidence brief explains a way to prepare a decision note from published material. It is original desk-based interpretation, not new incident research or a report of client results.

The reviewed sources demonstrate different kinds of evidence. Verizon's public 2026 DBIR hub presents breach findings and identifies its incident window as November 2024-October 2025. [1] NIST IR 8607, published in August 2026, summarises a workshop about a developing Cyber AI Profile; it is not itself a final implementation standard. [2]

The UK Cyber Governance Code of Practice, published in April 2025, is aimed primarily at boards and directors of medium and large organisations. [3] Its context should stay visible when considering a smaller Kenyan business. NIST's Generative AI Profile supports checking factual claims when AI assists research or drafting. [4]

The method below is GRCPreneur's proposed working routine. A reader should be able to trace each important claim and see which part of the recommendation depends on local assumptions.

From a cyber report to a management decision

Build a short evidence chain

Start with the decision

Write the question before collecting links. For example: should we approve a wider AI connection to client files, change a supplier arrangement or postpone a policy requirement? Identify the person with authority to make that decision.

Capture the source's actual claim

Record the publisher, title, version, publication date, reporting period, population and relevant passage. A publication year and an observation year are different fields. A workshop finding, technical recommendation and measured incident count also have different evidential roles.

Explain the connection to your business

State why the finding matters to the service under consideration. Identify what would need to be true locally for the recommendation to hold. An international pattern can justify a question about a dependency; it does not demonstrate a weakness in a specific customer's system.

Keep options and uncertainty together

Describe a small number of realistic options, their material benefits, remaining questions and constraints. If an important cost, permission or technical capability is unknown, mark it as needing confirmation. Do not replace a missing value with an unsupported estimate merely to complete a comparison.

End with a request that can be answered

Ask for a defined decision: approve a scoped trial, request further evidence, revise a proposal or defer subject to stated conditions. Include the responsible owner and the point at which the decision must be revisited.

From a cyber report to a management decision

Fictional example: permission to connect an AI tool

A small advisory team wants an AI tool to summarise approved reference documents. A proposal cites current AI research and asks for access to all client folders.

The reviewer separates the claims. Published guidance may explain risks and useful governance questions, but it does not establish which files this tool needs or whether the account terms permit their use. Those facts require a local check.

The decision note offers a narrower option: prepare a trial using approved, non-confidential material, with a named reviewer and no permission to send messages or alter records. It records the intended benefit, the output checks and the condition that would stop the trial. Any later access expansion needs another decision.

This is a fictional management example, not a claim that the suggested arrangement is sufficient for every use. It does not evaluate a named AI product or determine legal compliance.

The resulting note is more useful than a list of reports because the owner can see the request, its evidence, the missing facts and the authority needed for the next step.

From a cyber report to a management decision

Review before releasing the brief

Use this short final review:

- Does every material factual claim lead to a supporting passage?

- Are observation periods, populations and source limitations preserved?

- Are recommendations labelled as recommendations?

- Have business-specific assumptions been confirmed or clearly left open?

- Are the options and requested decision understandable without reading every source?

- Is there a named owner for the action and the next review?

The Professional Writing Brief and Review Workbook provides a place to record claim checks. The AI Use and Permission Decision Workbook can structure the specific connected-tool example.

For evidence about a supplier or customer, agree appropriate information handling before exchanging records. A public report should never become a reason to place confidential business material in a general enquiry form. The source list identifies the material reviewed, not endorsement of GRCPreneur.

Sources reviewed

[1] Verizon 2026 Data Breach Investigations Report: public report hub and takeaways

[2] NIST IR 8607: Cyber AI Profile Workshop #2 Summary

[3] UK DSIT: Cyber Governance Code of Practice

[4] NIST AI 600-1: Generative Artificial Intelligence Profile

Your next decision

Business question	
Decision owner	
Evidence still needed	
Next action / review	