

If the Cybersecurity Industry Profits from Cyberattacks, Why Do We Rely on Its Vendors to Tell Us How Secure We Are?

By: Jaiz Anuar

19 June 2026 · Cybersecurity · Digital Trust · 6 min read

The cybersecurity industry exists because cyber threats exist. The more complex, frequent, and damaging cyberattacks become, the more organisations spend on tools, platforms, consultants, assessments, intelligence, and managed services.

This creates an uncomfortable question: if the industry benefits from cyber insecurity, how much of its advice should we accept without challenge?

This is not an argument against cybersecurity vendors. Many vendors provide critical capabilities that organisations genuinely need. Security products, threat intelligence, incident response, monitoring, identity platforms, and assurance services are all important parts of modern defence.

However, it is a reminder that organisations must not outsource their judgement. Cybersecurity cannot be reduced to simply buying more tools, accepting more vendor recommendations, or treating every assessment finding as a purchasing justification.

The Incentive Problem

Every industry has incentives. A dentist earns money by treating dental problems, yet we still listen to dentists. The real issue is not whether professionals earn from problems. The issue is whether the advice is independent, proportionate, and in the best interest of the person receiving it.

The same applies to cybersecurity. A vendor may recommend more licences. A consultant may recommend another assessment. A platform provider may recommend deeper integration. A managed security provider may recommend extended monitoring coverage.

Each recommendation may be valid. But each recommendation also needs to be challenged.

Security or Dependency?

One of the biggest risks in modern cybersecurity is dependency disguised as maturity. Organisations may believe they are becoming more secure simply because they have more tools, more dashboards, more alerts, and more reports.

But maturity is not measured by the number of platforms deployed. It is measured by how well an organisation understands its risks, protects its critical assets, responds to threats, and makes informed decisions.

A tool can support security. It cannot replace ownership.

The Need for Independent Cyber Judgement

Organisations need internal capability to ask difficult questions. What risk are we actually reducing? Is this control addressing the root cause, or only adding another layer of visibility? Are we solving the problem, or subscribing to a permanent dependency?

Independent cyber judgement does not mean rejecting vendors. It means engaging vendors with clarity, confidence, and accountability.

Cyber leaders must be able to differentiate between real risk, perceived risk, compliance pressure, commercial persuasion, and technology hype.

Questions Worth Asking

Are we buying a solution because it reduces risk, or because it reduces anxiety?

Can we explain the business risk without using vendor language?

Are we addressing root causes, or only treating symptoms?

Do we have internal capability to challenge vendor recommendations?

Are our cybersecurity investments improving resilience, or increasing complexity?

Digital Trust Requires More Than Tools

Digital trust is not built through technology alone. It is built through governance, transparency, accountability, resilience, privacy, ethical decision-making, and the ability to make balanced risk-based decisions.

Tools are necessary. Vendors are necessary. External expertise is necessary. But none of them should become a substitute for internal responsibility.

The cybersecurity industry will continue to grow as cyber threats grow. That is reality. But organisations must avoid becoming passive consumers of fear.

Final Thought

The question is not whether we should trust cybersecurity vendors. The better question is whether we have built enough internal wisdom to know when to trust, when to challenge, and when to decide for ourselves.

Cybersecurity is not only about buying protection. It is about building judgement.