Three Reasons You Haven’t Been Hacked... Yet. Only One Is Good News.

By: Jaiz Anuar

25 June 2026 · Cybersecurity · Digital Trust · 7 min read

The absence of a known cyberattack may look like success. But silence can mean very different things.

There is a dangerous sentence often repeated in boardrooms, management meetings, and cybersecurity discussions:

“We have never been hacked.”

It sounds reassuring. It gives comfort to leadership. It seems to validate years of cybersecurity investment, governance papers, architecture reviews, audits, assessments, awareness programmes, and technology implementation.

But the uncomfortable question is this: does the absence of a known cyberattack really mean the organisation is secure?

Not necessarily.

The absence of a known breach is not proof of strong cybersecurity. It is only an observation. And like any observation, it can have more than one explanation.

In reality, there may be three reasons why an organisation has not been hacked. Only one of them is truly good news.

Reason One: Your Security Really Is Working

This is the explanation every organisation hopes is true. The organisation has invested properly in cybersecurity. Its architecture is well designed. Identity and access are governed. Privileged access is controlled. Systems are patched. Applications are tested. Monitoring is active. Incident response is ready. Governance is not only written in policy documents, but actually practised in daily decision-making.

In this scenario, attackers may have tried to enter the environment, but failed. Phishing emails were blocked. Malicious traffic was stopped. Weaknesses were remediated before they could be exploited. Suspicious activities were detected early. Controls worked as intended.

This is what cybersecurity maturity should look like. Not perfect protection, because perfect protection does not exist. But strong enough to increase the attacker’s cost, reduce their chance of success, and limit the damage if something goes wrong.

If this is the reason an organisation has not been hacked, then it is good news. The organisation has earned its confidence.

Reason Two: Nobody Has Chosen You Yet

The second explanation is less comforting. Perhaps the organisation has not been hacked simply because no serious attacker has decided to target it yet.

Cyber attackers do not always attack randomly. Many operate with their own version of business logic. They look for value. They look for weakness. They look for easy entry points. They compare effort against reward.

An organisation may remain untouched not because it is highly secure, but because it has not yet appeared attractive, vulnerable, or valuable enough to the right attacker.

That can change very quickly. A new digital service, a merger, a major public announcement, a regulatory issue, a new customer database, political attention, or even media exposure can suddenly change the organisation’s threat profile.

Yesterday’s silence may only mean the organisation was not interesting yesterday. It says very little about tomorrow.

This is why “we have never been hacked” can be a dangerous comfort. It may reflect maturity. But it may also reflect luck, timing, or lack of attacker interest.

Reason Three: You Have Already Been Compromised, But You Do Not Know It

The third explanation is the most uncomfortable.

The organisation may already be compromised, but the compromise has not yet been detected.

Not every attacker wants to create noise. Not every breach begins with ransomware. Not every intrusion immediately results in system outage, data leakage, or public embarrassment.

Some attackers prefer silence. They enter quietly, observe patiently, collect credentials, understand the environment, move carefully, and maintain access for as long as possible. The longer they remain undetected, the more valuable their position becomes.

In this scenario, the organisation may continue operating normally. Reports look clean. Dashboards look green. Vulnerability assessments may not show anything alarming. Penetration tests may close with no major findings. Audits may pass.

But none of those activities can fully prove that an attacker is absent. They only show what was tested, seen, or detected at a particular point in time.

This is where many organisations make a dangerous mistake. They confuse absence of evidence with evidence of absence.

The better question is not simply, “Have we been breached?”

The better question is, “How confident are we that we would know if we had been breached?”

The Same Silence Can Mean Different Things

This is the real problem. Three very different organisations can make the same statement: “We have never been hacked.”

One may be genuinely resilient. One may simply have been ignored. One may already be compromised without knowing it.

Same statement. Completely different truth.

That is why silence should never be treated as a cybersecurity metric. Silence is not proof of maturity. Silence is only the absence of known failure.

Final Thought

Cybersecurity is one of the few areas where success can look exactly like luck.

No incident. No headline. No ransomware. No crisis. No regulatory reporting. No public breach.

But silence alone tells us very little.

It may mean your security is working. It may mean attackers have not chosen you yet. Or it may mean someone is already inside, quietly making sure you do not notice.

The real challenge is not to say, “We have never been hacked.”

The real challenge is to understand why.

Question assumptions. Share knowledge. Build trust.