Three Types of Cybersecurity Confidence. Which One Does Your Organisation Have?

By: Jaiz Anuar

16 June 2026 · Cybersecurity · Leadership · Digital Trust · 8 min read

Every organisation believes it has confidence in its cybersecurity. The real question is whether that confidence is imagined, borrowed, or genuinely earned.

Boards receive reassuring dashboards. Executives hear that critical vulnerabilities have been remediated. Audit findings are closed. Penetration tests report no major issues. Security awareness programmes achieve impressive completion rates. Compliance certificates are renewed.

Everything appears to be under control.

Confidence is reassuring.

But confidence itself is not a security control.

More importantly, not all confidence is created equally.

Confidence comes in many forms.

Some confidence is imagined.

Some confidence is borrowed.

Very little confidence is truly earned.

The challenge for every organisation is understanding which type of confidence it actually possesses.

1. Imagined Confidence

Imagined confidence is built on assumptions rather than evidence.

It often sounds convincing because nothing appears to be wrong.

"We've never experienced a ransomware attack."

"Our systems have always been available."

"We've never had a major data breach."

"Our users complete their awareness training every year."

None of these statements are necessarily false.

The danger lies in the conclusion that often follows.

Therefore, we must be secure.

Silence becomes evidence.

Past success becomes proof.

The absence of known incidents becomes confidence.

But cybersecurity has never rewarded that logic.

An organisation may avoid attack because its controls are effective.

Or because attackers simply have not chosen it.

Or because a compromise remains undiscovered.

Imagined confidence grows quietly whenever organisations stop asking difficult questions.

Instead of asking, "How secure are we?", they begin asking, "Has anything bad happened?"

Those are not the same question.

The absence of bad news is comforting.

It is not evidence.

2. Borrowed Confidence

Borrowed confidence is more sophisticated.

Instead of relying on assumptions, organisations rely on someone else's assurance.

The latest penetration test reported no critical findings.

The external auditor was satisfied.

The cloud provider holds internationally recognised certifications.

The vendor assures that artificial intelligence is monitoring every threat.

The dashboard remains green month after month.

None of these things are without value.

Independent assessments, certifications, security technologies, and external expertise all play an important role in strengthening cybersecurity.

The problem begins when organisations stop thinking for themselves.

A penetration test demonstrates what was identified during a particular engagement.

It does not prove an attacker is absent.

A compliance audit measures conformity against defined requirements.

It does not guarantee operational resilience during a real attack.

A dashboard can only visualise the information it receives.

It cannot reveal what nobody is collecting.

Borrowed confidence is not necessarily wrong.

It simply becomes dangerous when external reassurance replaces internal understanding.

Eventually, organisations begin trusting reports more than they trust their own curiosity.

3. Earned Confidence

Earned confidence is different.

It is never assumed.

It is never inherited.

It is continuously demonstrated.

Organisations with earned confidence understand that every security control can fail.

Every identity can be compromised.

Every trusted device can become untrusted.

Every architecture decision carries assumptions that deserve regular review.

Because of this mindset, they deliberately challenge themselves.

They conduct tabletop exercises, not because they expect failure, but because they want to discover weaknesses before attackers do.

They validate backups by restoring them.

They regularly review privileged access instead of assuming it remains appropriate.

They perform red team exercises to test detection, response, and decision-making under pressure.

They question their own architecture.

They invite independent challenge.

Most importantly, they remain curious.

Ironically, organisations with earned confidence are often the least likely to claim they are completely secure.

They understand that confidence is not a destination.

It is a discipline.

Confidence Is Never Permanent

Cybersecurity is unlike many other disciplines.

Yesterday's confidence does not automatically survive tomorrow's technology.

Threat actors evolve.

Business models evolve.

Artificial intelligence evolves.

Supply chains evolve.

Confidence must evolve with them.

The moment confidence stops being challenged, it quietly begins to lose its value.

That is why mature organisations continuously validate not only their controls, but also the assumptions behind those controls.

Because every assumption has an expiry date.

The question is whether the organisation notices before an attacker does.

Questions Worth Asking

Is our confidence based on assumptions, external assurance, or continuous evidence?

Which security controls have we not tested recently?

If our confidence proved wrong tomorrow, how quickly would we know?

What assumptions have quietly become accepted facts?

Are we measuring security, or simply measuring the absence of visible failure?

Final Thought

Every organisation believes it has confidence in its cybersecurity.

The difference lies in where that confidence comes from.

Some confidence is imagined.

Some confidence is borrowed.

Very little confidence is earned.

The organisations most likely to remain resilient are not necessarily those with the biggest budgets, the newest technologies, or the most impressive dashboards.

They are the organisations that never become too comfortable with what they think they already know.

Because confidence should never replace curiosity.

It should be the reward for continuously challenging it.

So perhaps the most important question is not:

"How confident are we?"

Perhaps it is:

"Did we earn that confidence, or have we simply become comfortable believing it?"

Question assumptions. Share knowledge. Build trust.